XPort AR
User Guide

Part Number 900-405
Revision B November 2005

Copyright & Trademark

Contacts

Lantronix Corporate Headquarters
15353 Barranca Parkway
Irvine, CA 92618, USA
Phone: 949-453-3990
Fax: 949-453-3995

Technical Support
Phone: 800-422-7044 or 949-453-7198
Fax: 949-450-7226
Online: www.lantronix.com/support

Sales Offices
For a current list of our domestic and international sales offices, go to the Lantronix web site at www.lantronix.com/about/contact.

Disclaimer & Revisions

Note: *This product has been designed to comply with the limits for a Class B digital device pursuant to Part 15 of FCC and EN55022:1998 Rules when properly enclosed and grounded. These limits are designed to provide reasonable protection against radio interference in a residential installation. This equipment generates, uses, and can radiate radio frequency energy, and if not installed and used in accordance with this guide, may cause interference to radio communications*.

The information in this guide may change without notice. The manufacturer assumes no responsibility for any errors that may appear in this guide.

Date	Rev.	Comments
6/2005	A	Initial Document
11/2005	B	Added V2.0 software information

Contents

Figures

Tables

1: Using This Guide

Purpose and Audience

This guide provides the information needed to configure, use, and update the XPort AR™. It is intended for software developers and system integrators who are embedding the XPort AR in their designs.

Summary of Chapters

The remaining chapters in this guide include:

Chapter	Description
2: Description and Specifications	Main features of the product and the protocols it supports. Includes technical specifications.
3:Using DeviceInstaller	Instructions for viewing the current configuration using DeviceInstaller.
4:Configuration Using Web Manager	Instructions for accessing Web Manager and using it to configure settings for the XPort AR.
5:Configuration Using Telnet or Serial Port	Instructions for accessing Command Mode (the command line interface) using a Telnet connection through the network or through the serial port. Detailed information about the commands.
6:Point-to-Point Protocol (PPP)	Overviews PPP on the XPort AR.
7:Tunneling	Information on tunneling features available on the serial lines.
8:SSH and SSL Security	Overview and configuration of SSH and SSL security settings.
9:Using Email	Information on the SMTP server and setting email parameters on the XPort AR.
10:Configuration Pin Manager	Information on the Configuration Pin Manager (CPM) and setting the configurable pins to work with a device.
11:XML	Configuring the XPort AR using XML.
12:Branding the XPort AR	Instructions for customizing the XPort AR.
13:Updating Firmware	Instructions for obtaining the latest firmware and updating the XPort AR.
A: Technical Support	How to contact Lantronix Technical Support.
B: Binary to Hexadecimal	Instructions for converting binary values to hexadecimal and tables listing all configuration options in hexadecimal notation.

Additional Documentation

The following guides are available on the product CD or the Lantronix Web site (www.lantronix.com):

XPort AR Getting Started Provides the steps for getting the XPort AR evaluation board up and running.

XPort AR Integration Guide Provides information about the XPort AR hardware, testing the XPort AR using the evaluation board, and integrating the XPort AR into your product.

Com Port Redirector User Guide Provides information on using the Windows-based utility to create a virtual com port.

2: Description and Specifications

This chapter summarizes the XPort AR device server's features and basic information needed before getting started.

Features

The XPort AR is designed with additional features above and beyond the original XPort, including:

- The Evolution OS operating system
- Two full serial ports with all hardware handshaking signals or three serial ports without handshaking signals
- 11 configurable pins
- Supports fully compliant PoE designs by using PoE compliant magnetics and passing through both the used and unused pairs
- Increased memory: 4MB Flash and 1.25MB RAM
- Hardware capability in place to allow future software support for:
  - I2C Bus
  - SPI Bus
  - CAN Bus
  - USB
  - External interrupts, including one non-maskable
  - Timer input

Applications

The XPort AR device server connects serial devices such as those listed below to Ethernet networks using the IP protocol family.

- ATM machines
- CNC controllers
- Data collection devices
- Universal Power Supply (UPS) management units
- Telecommunications equipment
- Data display devices
- Security alarms and access control devices
- Handheld instruments
- Modems

- Time/attendance clocks and terminals

Protocol Support

The XPort AR device server contains a full-featured TCP/IP stack. Supported protocols include:

- ARP, IP, UDP, TCP, ICMP, BOOTP, DHCP, Auto IP, Telnet, FTP, TFTP, HTTP, SSH, SSL, SNMP, and SMTP for network communications and management.
- TCP, UDP, TCP/AES, UDP/AES, Telnet, and SSH for tunneling to the serial port.
- TFTP, FTP, and HTTP for firmware upgrades and uploading files.

Additional Features

Modem Emulation: In modem emulation mode, the XPort AR can replace dial-up modems. The unit accepts modem AT commands on the serial port, and then establishes a network connection to the end device, leveraging network connections and bandwidth to eliminate dedicated modems and phone lines.

Built-in Web Server: The XPort AR includes a built-in web server (Web Manager) for configuring the unit and displaying statistics.

Command Line Interface: A Command Line Interface (CLI) is available for configuration via the serial port or Telnet.

Configurable Pin Manager: The XPort AR contains a Configurable Pin Manager (CPM) accessible through the CLI or Web Manager to configure and manage the XPort AR's 11 configurable pins.

XML: To quickly configure multiple XPort AR units, export a configured XPort AR's configuration as an XML file. Import this file into other XPorts without having to repeat the configuration steps.

Power over Ethernet (PoE): The XPort AR supports PoE (also known as the IEEE standard 802.3af). Conventionally, network devices require a connection to the network and a power connection. PoE provides power to network devices over an Ethernet connection if the required hardware is available. The XPort AR passes PoE through the RJ45 to a connector on the bottom. To enable PoE, take the connections and design a PoE circuit and regulator to provide power for the device connected to the XPort AR. The XPort AR passes power not only through unused pairs, but through communications pairs as well.

Configuration Methods

After installation, the XPort AR requires configuration. For the unit to operate correctly on a network, it must have a unique IP address on the network. There are three basic methods for logging into the XPort AR and assigning IP addresses and other configurable settings:

DeviceInstaller: Configure the IP address and view network settings on the XPort AR using a Graphical User Interface (GUI) on a PC attached to a network. (See *3:Using DeviceInstaller*.)

Web Manager: Through a web browser, configure the XPort AR's settings using the Lantronix Web Manager. (See *4:Configuration Using Web Manager*.)

Command Mode: There are two methods to accessing Command Mode: making a Telnet connection or connecting a terminal (or a PC running a terminal emulation program) to the unit's serial port. (See *5:Configuration Using Telnet or Serial Port.)*

Addresses and Port Numbers

Hardware Address

The hardware address is also referred to as the Ethernet address or MAC address. The first three bytes of the Ethernet address are fixed and read 00-20-4A, identifying the unit as a Lantronix product. The fourth, fifth, and sixth bytes are unique numbers assigned to each unit.

Figure 2-1. Sample Hardware Address

```
00-20-4A-14-01-18 or 00:20:4A:14:01:18
```

IP Address

Every device connected to an IP network must have a unique IP address. This address references the specific unit.

Port Numbers

Every TCP connection and every UDP datagram is defined by a destination and source IP address, and a destination and source port number. For example, a Telnet server commonly uses port number 23.

The following is a list of the default server port numbers running on the XPort AR:

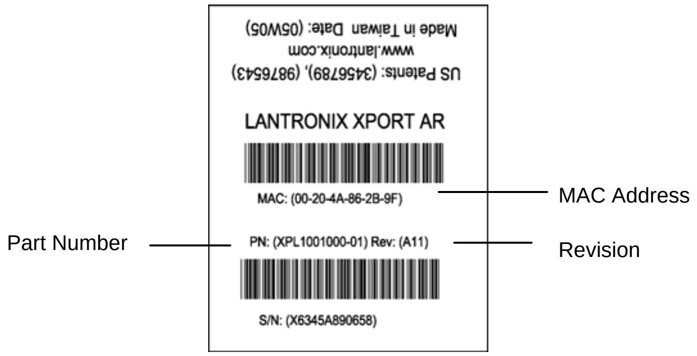
- TCP Port 22: SSH Server (Command Mode configuration)
- TCP Port 23: Telnet Server (Command Mode configuration)
- TCP Port 80: HTTP (Web Manager configuration)
- TCP Port 443: HTTPS (Web Manager configuration)
- UDP Port 161: SNMP
- TCP Port 21: FTP
- UDP Port 69: TFTP
- UDP Port 30718: 0x77FE Query port
- TCP/UDP Port 1001: Tunnel 1
- TCP/UDP Port 1002: Tunnel 2

Product Information Label

The product information label on the underside of the unit contains the following information about the specific unit:

- Bar code
- Serial number
- Product ID (name)
- Part number
- Hardware address (MAC address)

Figure 2-2. Product Label



3: Using DeviceInstaller

This chapter covers the steps for viewing the XPort AR device server's properties and device details.

Accessing XPort AR using DeviceInstaller

***Note:** Make note of the MAC address. It is needed to locate the XPort AR using DeviceInstaller.*

- Follow the instructions on the product CD to install and run DeviceInstaller.

1. Click **Start→Programs → Lantronix→DeviceInstaller→DeviceInstaller**.
2. Click on the XPort AR folder. The list of Lantronix XPort AR devices available displays.
3. Expand the list of XPorts by clicking the **+** symbol next to the XPort AR icon. Select the XPort AR unit by clicking on its IP address to view its configuration.

Viewing the XPort AR's Current Configuration

1. In the right window, click the **Device Details** tab. The current XPort AR configuration displays:

Name	Configurable field. Enter a **name** to identify the XPort AR. Double-click on the field, type in the value, and press **Enter** to complete. This name is not visible on other PCs or laptops using DeviceInstaller.
Group	Configurable field. Enter a **group** to categorize the XPort AR. Double-click on the field, type in the value, and press **Enter** to complete. This group name is not visible on other PCs or laptops using DeviceInstaller.
Comments	Configurable field. Enter **comments** for the XPort AR. Double-click on the field, type in the value, and press **Enter** to complete. This description or comment is not visible on other PCs or laptops using DeviceInstaller.
Device Family	Non-configurable field. Displays the XPort AR's device family type as **XPort AR**.
Type	Non-configurable field. Displays the device type as **XPort AR**.
ID	Non-configurable field. Displays the XPort AR's ID embedded within the box.
Hardware Address	Non-configurable field. Displays the XPort AR's hardware (or MAC) address.
Firmware Version	Non-configurable field. Displays the firmware currently installed on the XPort AR.

Extended Firmware Version	Provides additional information on the firmware version.
Online Status	Non-configurable field. Displays the XPort AR's status as online, offline, unreachable (the XPort AR is on a different subnet), or busy (the XPort AR is currently performing a task).
Telnet Enabled	Displays whether Telnet is enabled on this XPort AR.
Telnet Port	Non-configurable field. Displays the XPort AR's port for telnet sessions.
Web Enabled	Displays whether Web Manager access is enabled on this XPort AR.
WebPort	Non-configurable field. Displays the XPort AR's port for Web Manager configuration.
Maximum Baud Rate Supported	Non-configurable field. Displays the XPort AR's maximum baud rate. ***Note:*** *the XPort AR may not currently be running at this rate.*
Firmware Upgradeable	Non-configurable field. Displays **True**, indicating the XPort AR's firmware is upgradeable as newer version become available.
IP Address	Displays the XPort AR's current IP address. To change the IP address, click on the **Assign IP** button on the DeviceInstaller menu bar.
Supports Configurable Pins	Non-configurable field. Displays **True**, indicating configurable pins are available on the XPort AR.
Supports Email Triggers	Non-configurable field. Displays **True**, indicating email triggers are available on the XPort AR.

4: Configuration Using Web Manager

This chapter describes how to configure the XPort AR using Web Manager, Lantronix's browser-based configuration tool. The unit's configuration is stored in nonvolatile memory and is retained without power. All changes take effect immediately, unless otherwise noted.

Accessing Web Manager through a Web Browser

Log into the XPort AR using a standard Web browser.

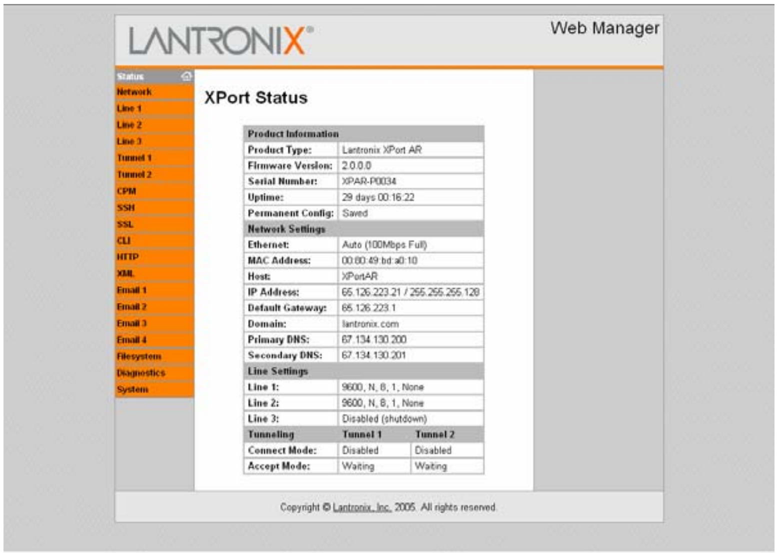
*Note: Alternatively, access the Web Manager by selecting the **Web Configuration** tab from DeviceInstaller.*

To access Web Manager:

1. Open a standard web browser (such as Netscape Navigator 6.x and above, Internet Explorer 5.5. and above, Mozilla Suite, Mozilla Firefox, or Opera).
2. Enter the IP address of the XPort AR in the address bar. The Web Manager home page displays.

Note: The XPort AR Status page (the home page) displays the common XPort AR configuration and product information.

Figure 4-1. Web Manager Home Page



XPort Status

Product Information		
Product Type:	Lantronix XPort AR	
Firmware Version:	2.0.0.0	
Serial Number:	XPAR-P0034	
Uptime:	29 days 00:16:22	
Permanent Config:	Saved	
Network Settings		
Ethernet:	Auto (100Mbps Full)	
MAC Address:	00:80:49:bd:a0:10	
Host:	XPortAR	
IP Address:	65.126.223.21 / 255.255.255.128	
Default Gateway:	65.126.223.1	
Domain:	lantronix.com	
Primary DNS:	67.134.130.200	
Secondary DNS:	67.134.130.201	
Line Settings		
Line 1:	9600, N, 8, 1, None	
Line 2:	9600, N, 8, 1, None	
Line 3:	Disabled (shutdown)	
Tunneling	**Tunnel 1**	**Tunnel 2**
Connect Mode:	Disabled	Disabled
Accept Mode:	Waiting	Waiting

Copyright © Lantronix, Inc. 2005. All rights reserved.

Network Settings

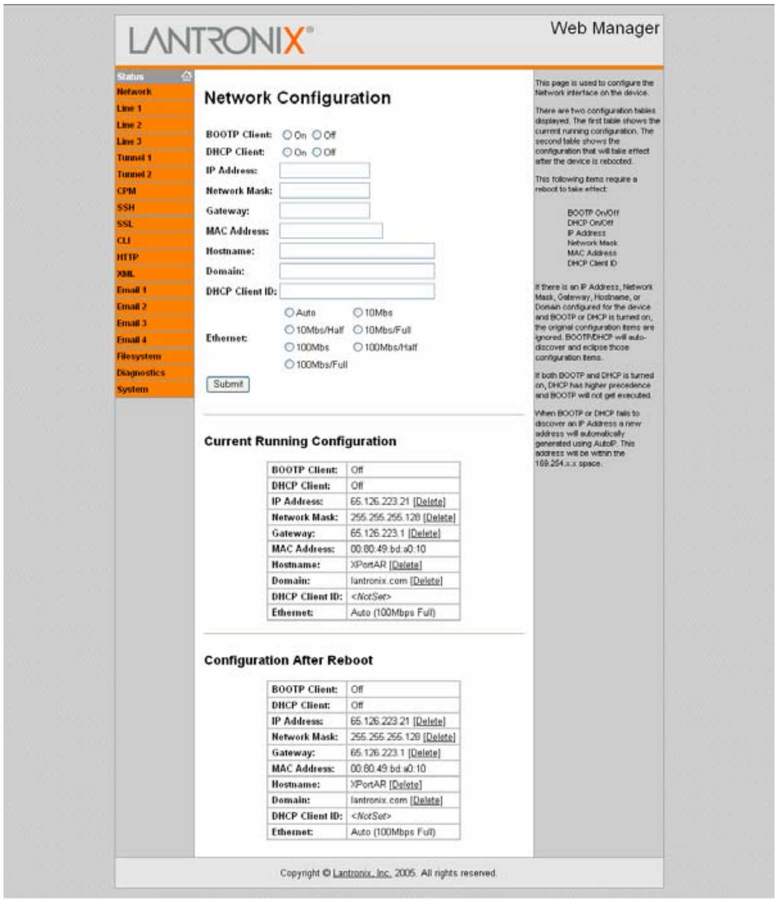
Click the **Network** link on the left navigation bar to display the Network menu. The sub-menus displayed allow for the configuration of the general network settings, protocol stack, DNS, SNMP, FTP, TFTP, IP address filter, and the query port.

Network Configuration

To configure the network's general configuration:

1. Click **Network → Configuration** from the navigation menu. The Network Configuration window displays.

Figure 4-2. Network Configuration



Network Configuration

BOOTP Client: ○ On ○ Off
DHCP Client: ○ On ○ Off
IP Address:
Network Mask:
Gateway:
MAC Address:
Hostname:
Domain:
DHCP Client ID:
Ethernet: ○ Auto ○ 10Mbs ○ 10Mbs/Half ○ 10Mbs/Full ○ 100Mbs ○ 100Mbs/Half ○ 100Mbs/Full

Current Running Configuration

BOOTP Client:	Off
DHCP Client:	Off
IP Address:	65.126.223.21 [Delete]
Network Mask:	255.255.255.128 [Delete]
Gateway:	65.126.223.1 [Delete]
MAC Address:	00:80:49:bd:a0:10
Hostname:	XPortAR [Delete]
Domain:	lantronix.com [Delete]
DHCP Client ID:	<NotSet>
Ethernet:	Auto (100Mbps Full)

Configuration After Reboot

BOOTP Client:	Off
DHCP Client:	Off
IP Address:	65.126.223.21 [Delete]
Network Mask:	255.255.255.128 [Delete]
Gateway:	65.126.223.1 [Delete]
MAC Address:	00:80:49:bd:a0:10
Hostname:	XPortAR [Delete]
Domain:	lantronix.com [Delete]
DHCP Client ID:	<NotSet>
Ethernet:	Auto (100Mbps Full)

This page is used to configure the Network interface on the device.

There are two configuration tables displayed. The first table shows the currrnt running configuration. The second table shows the configuration that will take effect after the device is rebooted.

This following items require a reboot to take effect:

BOOTP On/Off
DHCP On/Off
IP Address
Network Mask
MAC Address
DHCP Client ID

If there is an IP Address, Network Mask, Gateway, Hostname, or Domain configured for the device and BOOTP or DHCP is turned on, the original configuration items are ignored. BOOTP/DHCP will auto-discover and eclipse those configuration items.

If both BOOTP and DHCP is turned on, DHCP has higher precedence and BOOTP will not get executed.

When BOOTP or DHCP fails to discover an IP Address a new address will automatically generated using AutoIP. This address will be within the 169.254.x.x space.

Copyright © Lantronix, Inc. 2005. All rights reserved.

2. Enter or modify the following fields:

BOOTP Client	Select On or Off. Overrides the configured IP address, network mask, gateway, hostname, and domain. Note: When DHCP is set to On, the system automatically uses DHCP, regardless if BOOTP Client is set to On.
DHCP Client	Select On, Off, or Renew. Overrides the configured IP address, network mask, gateway, hostname, and domain.
IP Address	Enter the XPort AR's static IP address. The static address is used when BOOTP and DHCP are both set to Off.
Network Mask	Enter the XPort AR's network mask.
Gateway	Enter the XPort AR's gateway address.
MAC Address	Enter the XPort AR's new MAC address.
Hostname	Enter the unit's hostname.
Domain	Enter the unit's domain name.
DHCP Client ID	Enter the ID if a DHCP ID is used by the DHCP server. The DHCP server's lease table displays IP addresses and MAC addresses for devices. The lease table displays the Client ID, in hexadecimal notation, instead of the XPort AR's MAC address.
Ethernet	Select the speed for Ethernet transmission.

3. In the **Current Running Configuration** table, delete currently stored fields as necessary.

4. Click **Submit**. Changes are applied immediately to the XPort AR. Changes to the following settings require a reboot for the changes to take effect: DHCP, BOOTP, IP address, network mask, gateway, MAC address, and DHCP client ID.

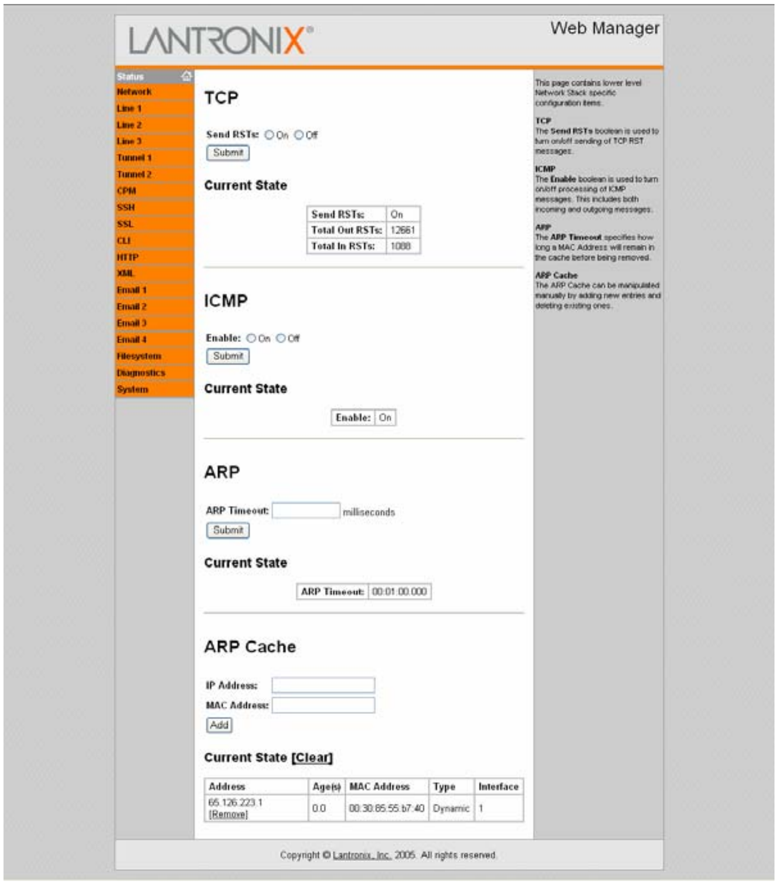
Note: *If DHCP or BOOTP fails, AutoIP intervenes and assigns an address. In this case, the static IP (if configured) is ignored.*

Protocol Stack Configuration

To configure the XPort AR's network stack protocols:

1. Click **Network → Protocol Stack** from the navigation menu. The Protocol Stack window displays the settings for TCP, ICMP, and ARP.

Figure 4-3. Protocol Stack



TCP

Send RSTs: ○ On ○ Off

Current State

Send RSTs:	On
Total Out RSTs:	12661
Total In RSTs:	1088

ICMP

Enable: ○ On ○ Off

Current State

Enable:	On

ARP

ARP Timeout: milliseconds

Current State

ARP Timeout:	00:01:00.000

ARP Cache

IP Address:

MAC Address:

Current State [Clear]

Address	Age(s)	MAC Address	Type	Interface
65.126.223.1 [Remove]	0.0	00:30:85:55:b7:40	Dynamic	1

This page contains lower level Network Stack specific configuration items.

TCP
The **Send RSTs** boolean is used to turn on/off sending of TCP RST messages.

ICMP
The **Enable** boolean is used to turn on/off processing of ICMP messages. This includes both incoming and outgoing messages.

ARP
The **ARP Timeout** specifies how long a MAC Address will remain in the cache before being removed.

ARP Cache
The ARP Cache can be manipulated manually by adding new entries and deleting existing ones.

Copyright © Lantronix, Inc. 2005. All rights reserved.

2. Enter or modify the following fields:

TCP

Send RSTs	TCP contains six control bits, with one or more defined in each packet. RST is one of the control bits. The RST bit is responsible for telling the receiving TCP stack to immediately end a connection. Sending this flag may pose a security risk. Select **Off** to disable the sending of the RST flag.

ICMP

Enable	*Internet Control Message Protocol (ICMP) can be used as an error-reporting protocol between two hosts. Commands such as ping use this protocol. Sending and processing ICMP messages may post a security risk.*

ARP

ARP Timeout	Enter the time, in milliseconds, for the ARP timeout. This is the duration an address remains in the cache.

ARP Cache

IP Address	Enter the IP address to add to the ARP table.
MAC Address	Enter the MAC address to add to the ARP table.

Note: Both the IP and MAC addresses are required for the ARP cache.

Current State

Clear	Select **Clear** to remove all entries in the ARP table.
Remove	Removes a specific entry from the ARP table.

3. Click **Submit** after each modified field. Changes are applied immediately to the XPort AR.

PPP

Point-to-Point Protocol (PPP) establishes a direct connection between two nodes. It defines a method for data link connectivity between devices using physical layers (such as serial lines).

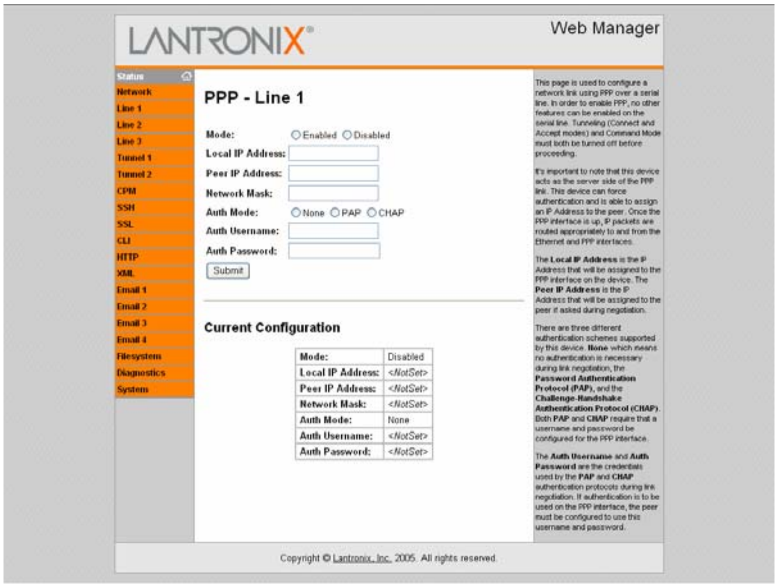
The XPort AR supports two types of PPP authorization: Password Authentication Protocol (PAP) and Challenge Handshake Protocol (CHAP). Both of these authentication methods require the configuration of a username and password. It also supports no authentication scheme when no authentication is required during link negotiation.

Note: The following section describes the steps to configure PPP 1 (PPP on serial line 1); these steps also apply to PPP 2.

To configure the XPort AR's PPP configuration:

1. Click **Network → PPP Line 1** from the navigation menu. The PPP – Line 1 window displays.

Figure 4-4. PPP Settings



PPP - Line 1

Mode: ○ Enabled ○ Disabled
Local IP Address:
Peer IP Address:
Network Mask:
Auth Mode: ○ None ○ PAP ○ CHAP
Auth Username:
Auth Password:

Current Configuration

Mode:	Disabled
Local IP Address:	<NotSet>
Peer IP Address:	<NotSet>
Network Mask:	<NotSet>
Auth Mode:	None
Auth Username:	<NotSet>
Auth Password:	<NotSet>

This page is used to configure a network link using PPP over a serial line. In order to enable PPP, no other features can be enabled on the serial line. Tunneling (Connect and Accept modes) and Command Mode must both be turned off before proceeding.

It's important to note that this device acts as the server side of the PPP link. This device can force authentication and is able to assign an IP Address to the peer. Once the PPP interface is up, IP packets are routed appropriately to and from the Ethernet and PPP interfaces.

The **Local IP Address** is the IP Address that will be assigned to the PPP interface on the device. The **Peer IP Address** is the IP Address that will be assigned to the peer if asked during negotiation.

There are three different authentication schemes supported by this device. **None** which means no authentication is necessary during link negotiation, the **Password Authentication Protocol (PAP)**, and the **Challenge-Handshake Authentication Protocol (CHAP)**. Both **PAP** and **CHAP** require that a username and password be configured for the PPP interface.

The **Auth Username** and **Auth Password** are the credentials used by the **PAP** and **CHAP** authentication protocols during link negotiation. If authentication is to be used on the PPP interface, the peer must be configured to use this username and password.

Copyright © Lantronix, Inc. 2005. All rights reserved.

2. Enter or modify the following fields:

Mode	Select **Enabled** to enable PPP on the XPort AR's serial line 1.
Local IP Address	Enter the IP address assigned to the device's PPP interface.

Peer IP Address	Enter the IP address assigned to the peer (when requested during negotiation).
Network Mask	Enter the network mask.
Auth. Mode	Choose the authentication mode. Select **None** when no authentication is required. Select **PAP** for Password Authentication Protocol. Select **CHAP** for the Challenge Handshake Authentication Protocol.

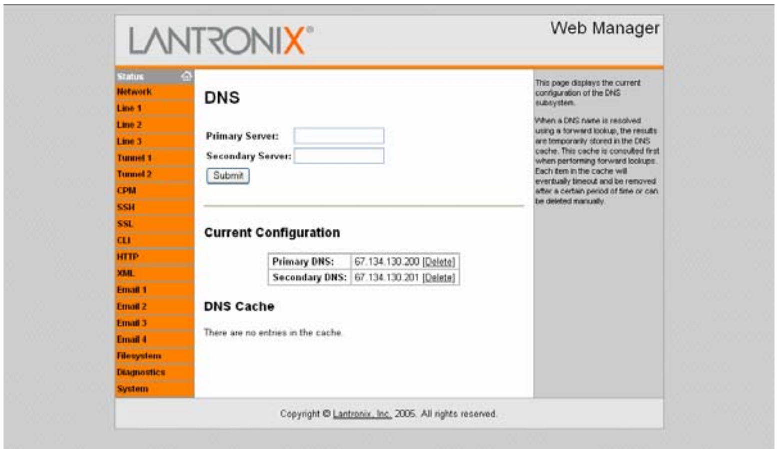
3. Click **Submit**. Changes are applied immediately to the XPort AR

DNS Configuration

To configure the XPort AR’s DNS configuration:

1. Click **Network → DNS** from the navigation menu. The DNS window displays.

Figure 4-5. DNS Settings



DNS

Primary Server:

Secondary Server:

Current Configuration

Primary DNS:	67.134.130.200 [Delete]
Secondary DNS:	67.134.130.201 [Delete]

DNS Cache

There are no entries in the cache.

This page displays the current configuration of the DNS subsystem.

When a DNS name is resolved using a forward lookup, the results are temporarily stored in the DNS cache. This cache is consulted first when performing forward lookups. Each item in the cache will eventually timeout and be removed after a certain period of time or can be deleted manually.

Copyright © Lantronix, Inc. 2005. All rights reserved.

2. Enter or modify the following fields:

DNS

Primary Server	Enter the DNS primary server address.
Secondary Server	Enter the DNS secondary server address.

Current Configuration

Primary Server	Displays the current **Primary Server** address. Select **Delete** to remove this value.
Secondary Server	Displays the current **Secondary Server** address. Select **Delete** to remove this value.

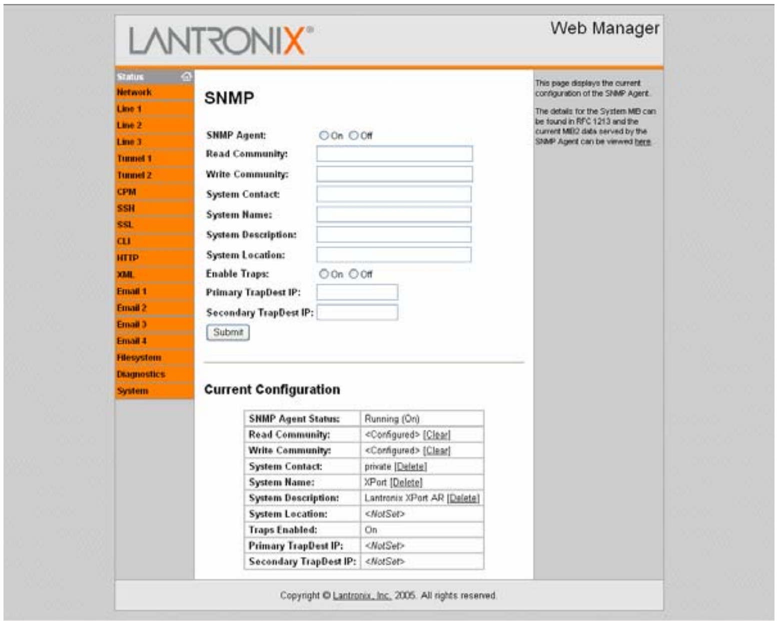
3. Click **Submit**. Changes are applied immediately to the XPort AR.

SNMP Configuration

To configure SNMP:

1. Click **Network → SNMP** from the navigation menu. The SNMP window opens and displays the current SNMP configuration.

Figure 4-6. SNMP Configuration



SNMP

SNMP Agent: ○ On ○ Off
Read Community:
Write Community:
System Contact:
System Name:
System Description:
System Location:
Enable Traps: ○ On ○ Off
Primary TrapDest IP:
Secondary TrapDest IP:

Current Configuration

SNMP Agent Status:	Running (On)
Read Community:	<Configured> [Clear]
Write Community:	<Configured> [Clear]
System Contact:	private [Delete]
System Name:	XPort [Delete]
System Description:	Lantronix XPort AR [Delete]
System Location:	<NotSet>
Traps Enabled:	On
Primary TrapDest IP:	<NotSet>
Secondary TrapDest IP:	<NotSet>

This page displays the current configuration of the SNMP Agent.

The details for the System MIB can be found in RFC 1213 and the current MIB2 data served by the SNMP Agent can be viewed here.

Copyright © Lantronix, Inc. 2005. All rights reserved.

2. Enter or modify the following fields:

SNMP Agent	Select **On** to enable SNMP.
Read Community	Enter the SNMP read-only community string.
Write Community	Enter the SNMP read/write community string.
System Contact	Enter the name of the system contact.
System Name	Enter the system name.
System Description	Enter the system description.
System Location	Enter the system location.
Enable Traps	Select **On** to enable the transmission of the SNMP cold start trap messages. This trap is generated during system boot.
Primary TrapDest IP	Enter the primary SNMP trap host.
Secondary TrapDest IP	Enter the secondary SNMP trap host.

3. In the **Current Configuration** table, delete and clear currently stored fields as necessary.

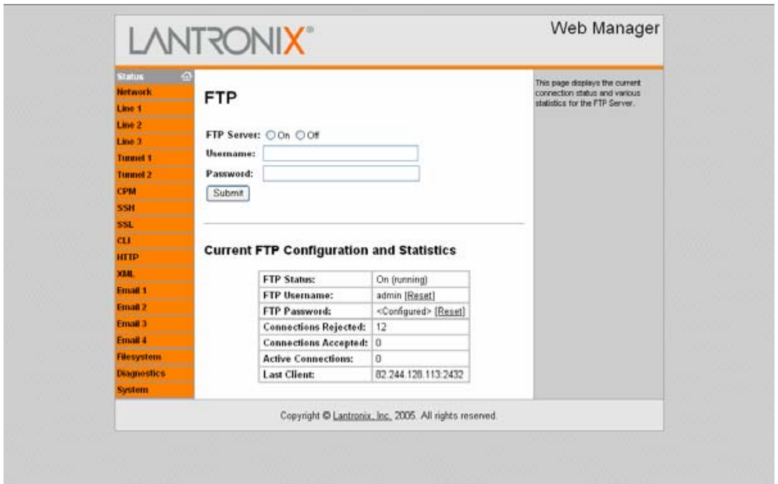
4. Click **Submit**. Changes are applied immediately to the XPort AR.

FTP Configuration

To configure FTP:

1. Click **Network → FTP** from the navigation menu. The FTP window opens to display the current configuration.

Figure 4-7. FTP Configuration



FTP

FTP Server: ○ On ○ Off

Username:

Password:

Current FTP Configuration and Statistics

FTP Status:	On (running)
FTP Username:	admin [Reset]
FTP Password:	<Configured> [Reset]
Connections Rejected:	12
Connections Accepted:	0
Active Connections:	0
Last Client:	82.244.128.113:2432

This page displays the current connection status and various statistics for the FTP Server.

Copyright © Lantronix, Inc. 2005. All rights reserved.

2. Enter or modify the following fields:

FTP

FTP Server	Select **On** to enable the FTP server.
Username	Enter the username to use when logging in via FTP.
Password	Enter the password to use when logging in via FTP.

3. In the **Current FTP Configuration and Statistics** tables, reset currently stored fields as necessary by clicking the **Reset** link.

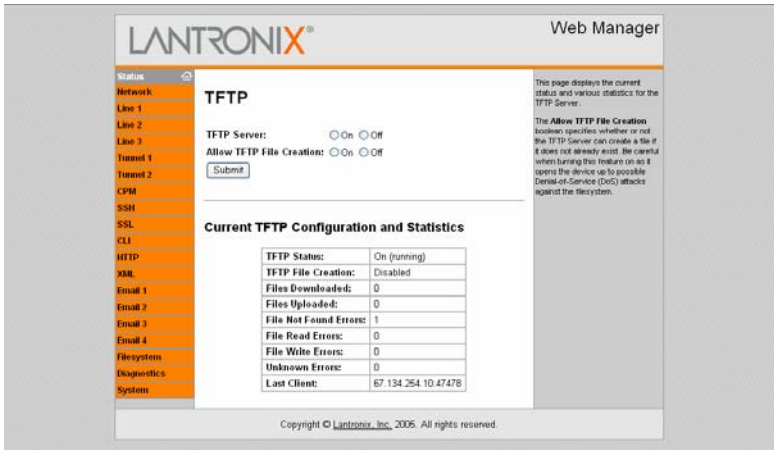
4. Click **Submit**. Changes are applied immediately to the XPort AR.

TFTP Configuration

To configure TFTP:

1. Click **Network → TFTP** from the navigation menu. The TFTP window opens to display the current configuration.

Figure 4-8. TFTP Configuration



TFTP

TFTP Server: ○ On ○ Off

Allow TFTP File Creation: ○ On ○ Off

Current TFTP Configuration and Statistics

TFTP Status:	On (running)
TFTP File Creation:	Disabled
Files Downloaded:	0
Files Uploaded:	0
File Not Found Errors:	1
File Read Errors:	0
File Write Errors:	0
Unknown Errors:	0
Last Client:	67.134.254.10:47478

This page displays the current status and various statistics for the TFTP Server.

The **Allow TFTP File Creation** boolean specifies whether or not the TFTP Server can create a file if it does not already exist. Be careful when turning this feature on as it opens the device up to possible Denial-of-Service (DoS) attacks against the filesystem.

Copyright © Lantronix, Inc. 2005. All rights reserved.

2. Enter or modify the following fields:

TFTP

TFTP Server	Select **On** to enable the FTP server.
Allow TFTP File Creation	Enable the automatic creation of files stored by the TFTP server.

3. In the **Current TFTP Configuration and Statistics** table, reset currently stored fields as necessary by clicking the **Reset** link.

4. Click **Submit**. Changes are applied immediately to the XPort AR.

IP Address Filter

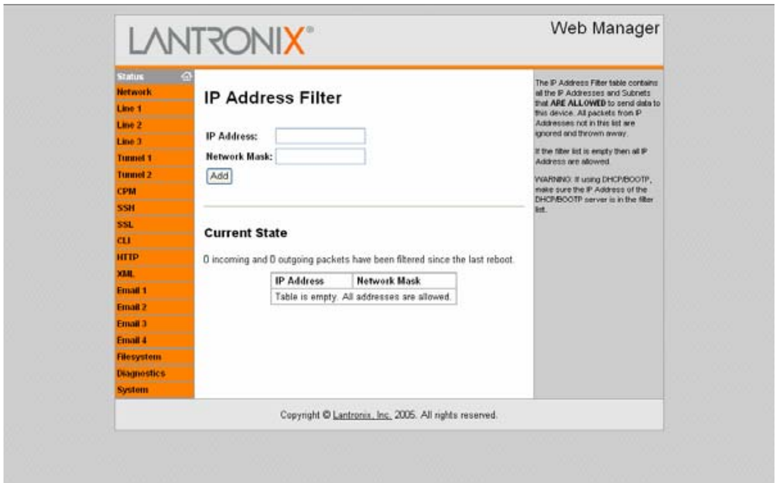
The IP address filter specifies the hosts and subnets permitted to communicate with the XPort AR.

Note: If using DHCP/BOOTP, ensure the DHCP/BOOTP server is in this list.

To configure the IP address filter:

1. Click **Network → IP Address Filter** from the navigation menu. The IP Address Filter window opens to display the current configuration.

Figure 4-9. IP Address Filter Configuration



IP Address Filter

IP Address:

Network Mask:

Current State

0 incoming and 0 outgoing packets have been filtered since the last reboot.

IP Address	Network Mask
Table is empty. All addresses are allowed.	

The IP Address Filter table contains all the IP Addresses and Subnets that **ARE ALLOWED** to send data to this device. All packets from IP Addresses not in this list are ignored and thrown away.

If the filter list is empty then all IP Address are allowed.

WARNING: If using DHCP/BOOTP, make sure the IP Address of the DHCP/BOOTP server is in the filter list.

Copyright © Lantronix, Inc. 2005. All rights reserved.

2. Enter or modify the following fields:

IP Address	Enter the IP address to add to the IP filter table.
Network Mask	Enter the IP address' network mask in dotted notation.

3. In the **Current State** table, click **Remove** to delete fields as necessary.

4. Click **Submit**. Changes are applied immediately to the XPort AR.

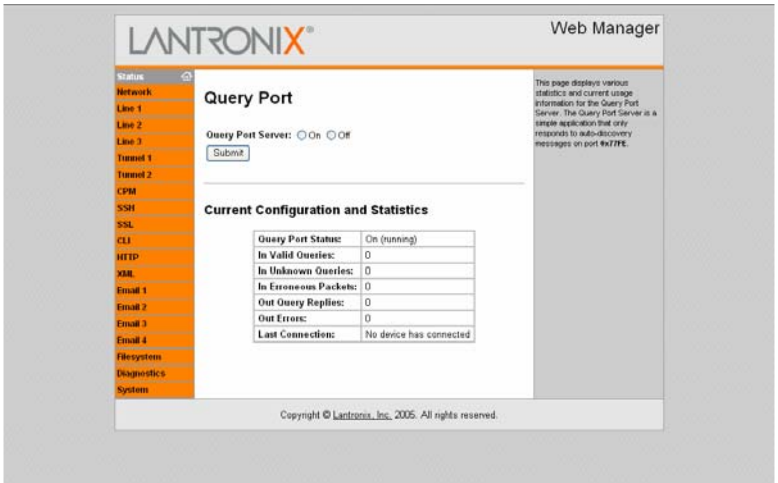
Query Port

The query port (0x77FE) is used for the automatic discovery of the device by the DeviceInstaller utility. Only 0x77FE discover messages from DeviceInstaller are supported. For more information on DeviceInstaller, see *Using DeviceInstaller* on page 15.

To configure the query port server:

1. Click **Network → Query Port** from the navigation menu. The Query Port window opens to display the current configuration.

Figure 4-10. Query Port Configuration



Query Port

Query Port Server: ○ On ○ Off

Current Configuration and Statistics

Query Port Status:	On (running)
In Valid Queries:	0
In Unknown Queries:	0
In Erroneous Packets:	0
Out Query Replies:	0
Out Errors:	0
Last Connection:	No device has connected

This page displays various statistics and current usage information for the Query Port Server. The Query Port Server is a simple application that only responds to auto-discovery messages on port 0x77FE.

Copyright © Lantronix, Inc. 2005. All rights reserved.

2. Select **On** to enable the query port server.

3. Click **Submit**. Changes are applied immediately to the XPort AR.

Line 1, Line 2, and Line 3 Settings

Select the **Line 1**, **Line 2**, or **Line 3** link on the left menu bar to display the **Line** menu. The sub-menus allow for both general configuration and command mode configuration.

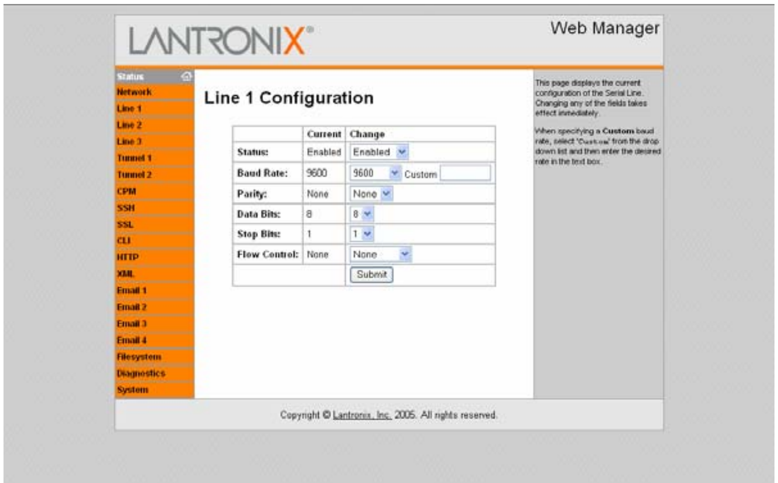
Note: *The following section describes the steps to configure Line 1; these steps also apply to Line 2 and Line 3 menu options*.

Line 1 Configuration

To configure Line 1:

1. Click **Line 1 → Configuration** from the navigation menu. The Line 1 Configuration window displays.

Figure 4-11. Line 1 Configuration



Line 1 Configuration

	Current	Change
Status:	Enabled	Enabled
Baud Rate:	9600	9600 Custom
Parity:	None	None
Data Bits:	8	8
Stop Bits:	1	1
Flow Control:	None	None

This page displays the current configuration of the Serial Line. Changing any of the fields takes effect immediately.

When specifying a **Custom** baud rate, select 'Custom' from the drop down list and then enter the desired rate in the text box.

Copyright © Lantronix, Inc. 2005. All rights reserved.

2. Enter or modify the following fields:

Status	Displays the whether the current line is enabled. To change the status, select **Enabled** or **Disabled** from the pull-down menu.
Baud Rate	Select the XPort AR's baud rate from the pull-down menu. The default is **9600**.
Parity	Select the XPort AR's parity from the pull-down menu. The default is **None.**
Data Bits	Select the number of data bits from the pull-down menu. The default is **8**.
Stop Bits	Select the number of stop bits from the pull-down menu. The default is **1.**
Flow Control	Select the XPort AR's flow control from the pull-down menu. The default is **None.**

3. Click **Submit**. Changes are applied immediately to the XPort AR.

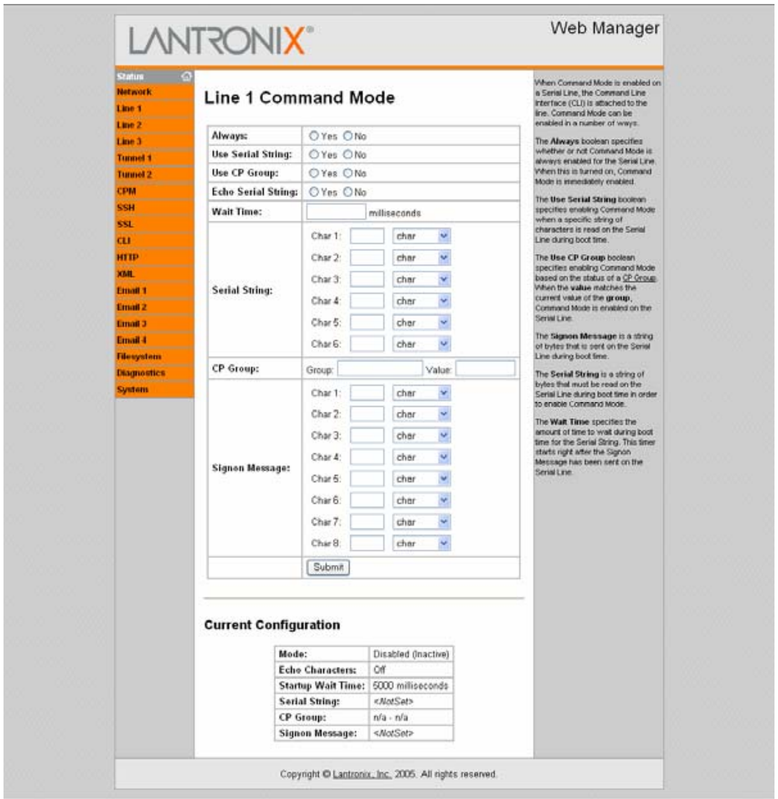
Line 1 Command Mode

Setting Command Mode enables the CLI on the serial line.

To configure Line 1's command mode:

1. Click **Line 1 → Command Mode** from the navigation menu. The Line 1 Command Mode window displays.

Figure 4-12. Line 1 Command Mode



Line 1 Command Mode

Always:	○ Yes ○ No
Use Serial String:	○ Yes ○ No
Use CP Group:	○ Yes ○ No
Echo Serial String:	○ Yes ○ No
Wait Time:	milliseconds
Serial String:	Char 1: char Char 2: char Char 3: char Char 4: char Char 5: char Char 6: char
CP Group:	Group: Value:
Signon Message:	Char 1: char Char 2: char Char 3: char Char 4: char Char 5: char Char 6: char Char 7: char Char 8: char

Current Configuration

Mode:	Disabled (inactive)
Echo Characters:	Off
Startup Wait Time:	5000 milliseconds
Serial String:	<NotSet>
CP Group:	n/a - n/a
Signon Message:	<NotSet>

When Command Mode is enabled on a Serial Line, the Command Line Interface (CLI) is attached to the line. Command Mode can be enabled in a number of ways.

The **Always** boolean specifies whether or not Command Mode is always enabled for the Serial Line. When this is turned on, Command Mode is immediately enabled.

The **Use Serial String** boolean specifies enabling Command Mode when a specific string of characters is read on the Serial Line during boot time.

The **Use CP Group** boolean specifies enabling Command Mode based on the status of a CP Group. When the **value** matches the current value of the **group**, Command Mode is enabled on the Serial Line.

The **Signon Message** is a string of bytes that is sent on the Serial Line during boot time.

The **Serial String** is a string of bytes that must be read on the Serial Line during boot time in order to enable Command Mode.

The **Wait Time** specifies the amount of time to wait during boot time for the Serial String. This timer starts right after the Signon Message has been sent on the Serial Line.

Copyright © Lantronix, Inc. 2005. All rights reserved.

2. Enter or modify the following fields:

Always	Select **Yes** to enable the XPort AR's command mode.
Use Serial String	Select **Yes** to start command mode based on a serial string.
Use CP Group	Select **Yes** to start command mode based on the value of a CP group.
Echo Serial String	Select **Yes** to enable echoing of the serial string at boot-up.
Wait Time	Enter the wait time for the serial string during boot-up.
Serial String	In the **Char** field, enter the serial string characters. Select the string type from the pull down menu as **Character**, **Binary**, or **Decimal** notation.
CP Group	Enter the CP group name and its value.
Signon Message	In the **Char** field, enter the boot-up signon message. Select the string type from the pull down menu as **Character**, **Binary**, or **Decimal** notation.

3. In the **Current Configuration** table, clear currently stored fields as necessary.

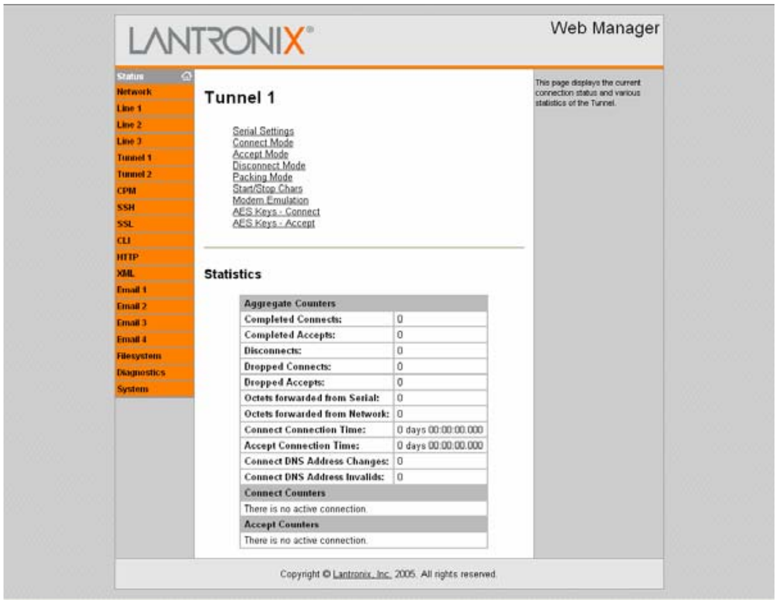
4. Click **Submit**. Changes are applied immediately to the XPort AR.

Tunnel 1 and Tunnel 2 Settings

Select the **Tunnel 1** or **Tunnel 2** link on the left menu bar to display the **Tunnel** menu. The sub-menus allow for the configuration of serial settings, connect mode, accept mode, disconnect mode, packing mode, start and stop characters, and modem emulation.

Note: The following section describes the steps to configure Tunnel 1; these steps also apply to Tunnel 2 menu options.

Figure 4-13. Tunnel 1



Tunnel 1

Serial Settings
Connect Mode
Accept Mode
Disconnect Mode
Packing Mode
Start/Stop Chars
Modem Emulation
AES Keys - Connect
AES Keys - Accept

Statistics

Aggregate Counters	
Completed Connects:	0
Completed Accepts:	0
Disconnects:	0
Dropped Connects:	0
Dropped Accepts:	0
Octets forwarded from Serial:	0
Octets forwarded from Network:	0
Connect Connection Time:	0 days 00:00:00.000
Accept Connection Time:	0 days 00:00:00.000
Connect DNS Address Changes:	0
Connect DNS Address Invalids:	0
Connect Counters	
There is no active connection.	
Accept Counters	
There is no active connection.	

This page displays the current connection status and various statistics of the Tunnel.

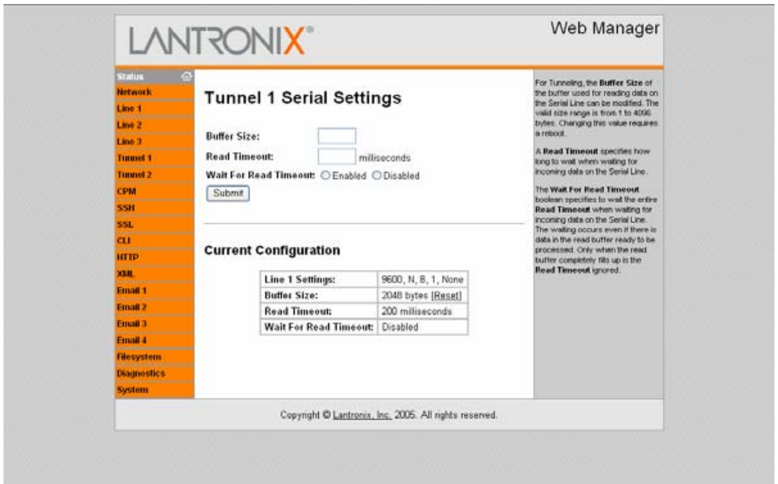
Copyright © Lantronix, Inc. 2005. All rights reserved.

Serial Settings

To configure serial settings:

1. Click **Tunnel 1 → Serial Settings** from the navigation menu. The Tunnel 1 Serial Settings window displays.

Figure 4-14. Tunnel 1 Serial Settings



Tunnel 1 Serial Settings

Buffer Size:
Read Timeout: milliseconds
Wait For Read Timeout: ○ Enabled ○ Disabled

Current Configuration

Line 1 Settings:	9600, N, 8, 1, None
Buffer Size:	2048 bytes [Reset]
Read Timeout:	200 milliseconds
Wait For Read Timeout:	Disabled

For Tunneling, the **Buffer Size** of the buffer used for reading data on the Serial Line can be modified. The valid size range is from 1 to 4096 bytes. Changing this value requires a reboot.

A **Read Timeout** specifies how long to wait when waiting for incoming data on the Serial Line.

The **Wait For Read Timeout** boolean specifies to wait the entire **Read Timeout** when waiting for incoming data on the Serial Line. The waiting occurs even if there is data in the read buffer ready to be processed. Only when the read buffer completely fills up is the **Read Timeout** ignored.

Copyright © Lantronix, Inc. 2005. All rights reserved.

2. Enter or modify the following fields:

Buffer Size	Enter the buffer size used for the tunneling of data received.
Read Timeout	Enter the time, in milliseconds, for tunneling wait for serial data
Wait for Read Timeout	Select **Enabled** to cause the tunneling to wait for a read timeout before returning serial data.

3. In the **Current Configuration** table, reset currently stored fields as necessary.

4. Click **Submit**. Changes are applied immediately to the XPort AR.

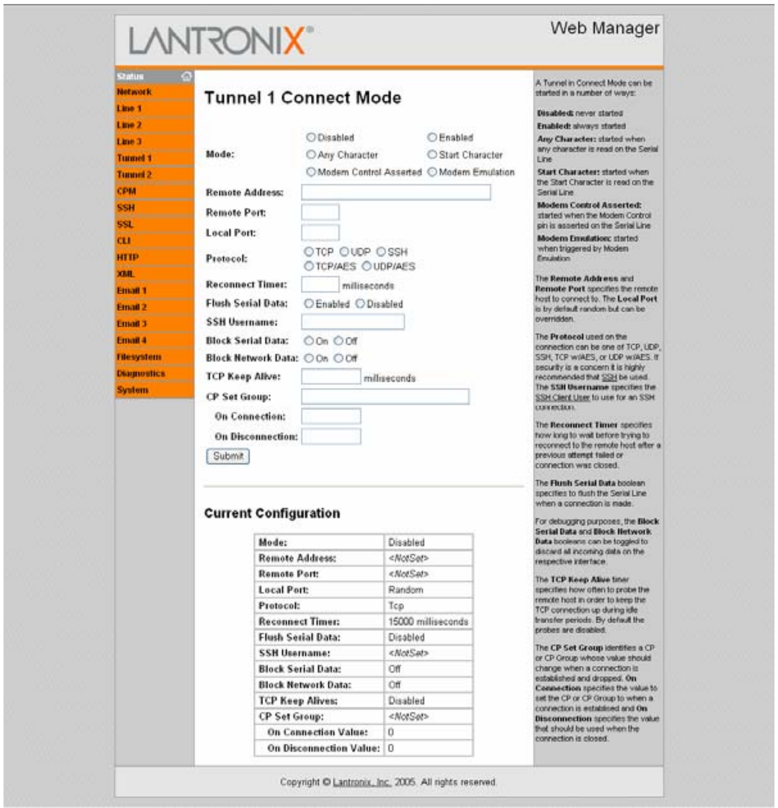
Connect Mode

Connect mode defines how the unit makes an outgoing connection.

To configure Tunnel 1's connect mode:

1. Select **Tunnel 1 → Connect Mode** from the navigation menu. The Tunnel 1 Connect Mode window displays.

Figure 4-15. Tunnel 1 Connect Mode



Tunnel 1 Connect Mode

Mode: ○ Disabled ○ Enabled ○ Any Character ○ Start Character ○ Modem Control Asserted ○ Modem Emulation

Remote Address:

Remote Port:

Local Port:

Protocol: ○ TCP ○ UDP ○ SSH ○ TCP/AES ○ UDP/AES

Reconnect Timer: milliseconds

Flush Serial Data: ○ Enabled ○ Disabled

SSH Username:

Block Serial Data: ○ On ○ Off

Block Network Data: ○ On ○ Off

TCP Keep Alive: milliseconds

CP Set Group:

On Connection:

On Disconnection:

Current Configuration

Mode:	Disabled
Remote Address:	*<NotSet>*
Remote Port:	*<NotSet>*
Local Port:	Random
Protocol:	Tcp
Reconnect Timer:	15000 milliseconds
Flush Serial Data:	Disabled
SSH Username:	*<NotSet>*
Block Serial Data:	Off
Block Network Data:	Off
TCP Keep Alives:	Disabled
CP Set Group:	*<NotSet>*
On Connection Value:	0
On Disconnection Value:	0

A Tunnel in Connect Mode can be started in a number of ways:

Disabled: never started

Enabled: always started

Any Character: started when any character is read on the Serial Line

Start Character: started when the Start Character is read on the Serial Line

Modem Control Asserted: started when the Modem Control pin is asserted on the Serial Line

Modem Emulation: started when triggered by Modem Emulation

The **Remote Address** and **Remote Port** specifies the remote host to connect to. The **Local Port** is by default random but can be overridden.

The **Protocol** used on the connection can be one of TCP, UDP, SSH, TCP w/AES, or UDP w/AES. If security is a concern it is highly recommended that SSH be used. The **SSH Username** specifies the SSH Client User to use for an SSH connection.

The **Reconnect Timer** specifies how long to wait before trying to reconnect to the remote host after a previous attempt failed or connection was closed.

The **Flush Serial Data** boolean specifies to flush the Serial Line when a connection is made.

For debugging purposes, the **Block Serial Data** and **Block Network Data** booleans can be toggled to discard all incoming data on the respective interface.

The **TCP Keep Alive** timer specifies how often to probe the remote host in order to keep the TCP connection up during idle transfer periods. By default the probes are disabled.

The **CP Set Group** identifies a CP or CP Group whose value should change when a connection is established and dropped. **On Connection** specifies the value to set the CP or CP Group to when a connection is estabiloed and **On Disconnection** specifies the value that should be used when the connection is closed.

Copyright © Lantronix, Inc. 2005. All rights reserved.

2. Enter or modify the following fields:

Mode	Select **Disabled** to turn off connect mode. **Any Character** enables connect mode upon receiving a character. **Start Character** enables connect mode upon receiving the start character. Select **DSR Active** to enable Connect Mode if Data Set Ready (DSR) pin is active on the serial line. Select **Modem Emulation** to use modem emulation on this tunnel.
Remote Address	Enter the remote address to which the XPort AR will connect. Enter an IP address or DNS name.
Remote Port	Enter the remote port number.
Local Port	Enter the port for use as the local port. A random port is selected by default.
Protocol	Select the protocol type for use in command mode. TCP is the default protocol.
Reconnect Timer	Enter the reconnect time in milliseconds. The XPort AR attempts to reconnect this amount of time after failing a connection or exiting an existing connection.
SSH Username	Enter the SSH username. The tunnel uses the SSH keys for the client username.
Block Serial Data	Select **On** to block (not tunnel) serial data transmitted to the XPort AR.
Block Network Data	Select **On** to block (not tunnel) network data transmitted to the XPort AR.
TCP Keep Alive	Enter the time, in milliseconds, the unit waits during a silent connection before checking if the currently connected network device is still on the network. If the unit then gets no response after 8 attempts, it drops that connection.
CP Set Group	Identifies a CP or CP Group whose value should change when a connection is established and dropped.
On Connection	Specifies the value to set the CP or CP Group when a connection is established.
On Disconnection	Specifies the value used when the connection is closed.

3. Click **Submit**. Changes are applied immediately to the XPort AR.

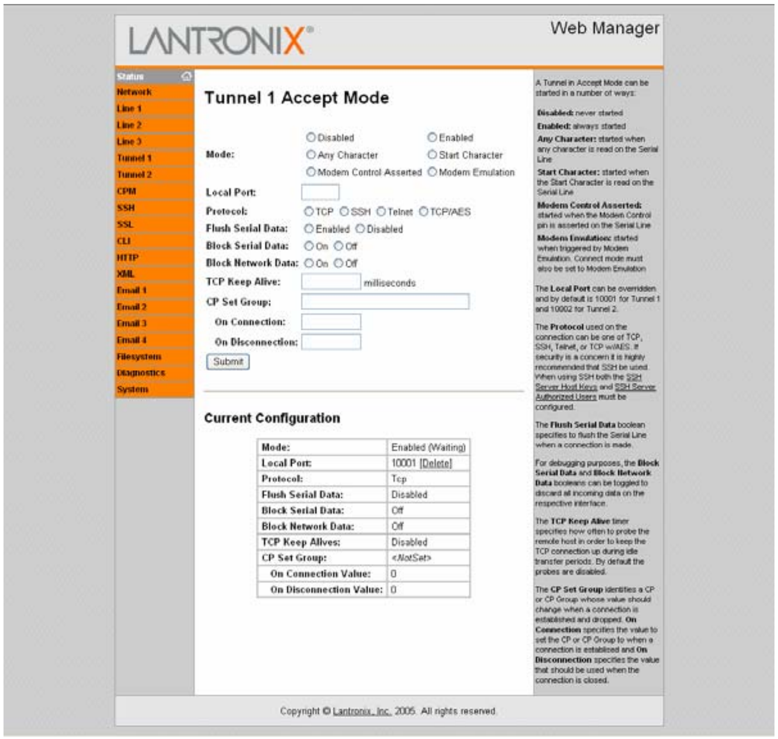
Accept Mode

In accept mode, the XPort AR listens (waits) for incoming connections.

To configure the tunnel's accept mode:

1. Click **Tunnel 1 → Accept Mode** from the navigation menu. The Tunnel 1 Accept Mode window displays.

Figure 4-16. Tunnel 1 Accept Mode



Tunnel 1 Accept Mode

Mode: ○ Disabled ○ Enabled ○ Any Character ○ Start Character ○ Modem Control Asserted ○ Modem Emulation

Local Port:

Protocol: ○ TCP ○ SSH ○ Telnet ○ TCP/AES

Flush Serial Data: ○ Enabled ○ Disabled

Block Serial Data: ○ On ○ Off

Block Network Data: ○ On ○ Off

TCP Keep Alive: milliseconds

CP Set Group:

On Connection:

On Disconnection:

Submit

Current Configuration

Mode:	Enabled (Waiting)
Local Port:	10001 [Delete]
Protocol:	Tcp
Flush Serial Data:	Disabled
Block Serial Data:	Off
Block Network Data:	Off
TCP Keep Allves:	Disabled
CP Set Group:	<NotSet>
On Connection Value:	0
On Disconnection Value:	0

A Tunnel in Accept Mode can be started in a number of ways:

Disabled: never started

Enabled: always started

Any Character: started when any character is read on the Serial Line

Start Character: started when the Start Character is read on the Serial Line

Modem Control Asserted: started when the Modem Control pin is asserted on the Serial Line

Modem Emulation: started when triggered by Modem Emulation. Connect mode must also be set to Modem Emulation

The **Local Port** can be overridden and by default is 10001 for Tunnel 1 and 10002 for Tunnel 2.

The **Protocol** used on the connection can be one of TCP, SSH, Telnet, or TCP w/AES. If security is a concern it is highly recommended that SSH be used. When using SSH both the SSH Server Host Keys and SSH Server Authorized Users must be configured.

The **Flush Serial Data** boolean specifies to flush the Serial Line when a connection is made.

For debugging purposes, the **Block Serial Data** and **Block Network Data** booleans can be toggled to discard all incoming data on the respective interface.

The **TCP Keep Alive** timer specifies how often to probe the remote host in order to keep the TCP connection up during idle transfer periods. By default the probes are disabled.

The **CP Set Group** identifies a CP or CP Group whose value should change when a connection is established and dropped. **On Connection** specifies the value to set the CP or CP Group to when a connection is establised and **On Disconnection** specifies the value that should be used when the connection is closed.

Copyright © Lantronix, Inc. 2005. All rights reserved.

2. Enter or modify the following fields:

Mode	Select **Disabled** to disable Accept Mode completely. Select **Enable** to enable Accept Mode at all times. Select **Any Character** to enable Accept Mode upon receiving any character or select **Start Character** to enable Accept Mode upon receiving the start character. Select **DSR Active** to enable Accept Mode if the Data Set Ready (DSR) pin is active on the serial line. In general, a modem sends a DSR signal to its attached computer to indicate that the modem is ready to operate.
Local Port	Enter the port number for use as the local port. The default is port 10001.
Protocol	Select the protocol type for use with Accept Mode. The default protocol is TCP.
Flush Serial Data	Select **Enabled** to flush the serial data buffer on a new connection.
Block Serial Data	Select **On** to block, or not tunnel, serial data transmitted to the XPort AR.
Block Network Data	Select **On** to block, or not tunnel, network data transmitted to the XPort AR.
TCP Keep Alive	Enter the time, in milliseconds, the unit waits during a silent connection before checking if the currently connected network device is still on the network. If the unit then gets no response after 8 attempts, it drops that connection.
CP Set Group	Identifies a CP or CP Group whose value should change when a connection is established and dropped.

On Connection	Specifies the value to set the CP or CP Group when a connection is established.
On Disconnection	Specifies the value used when the connection is closed.

3. Click **Submit**. Changes are applied immediately to the XPort AR.

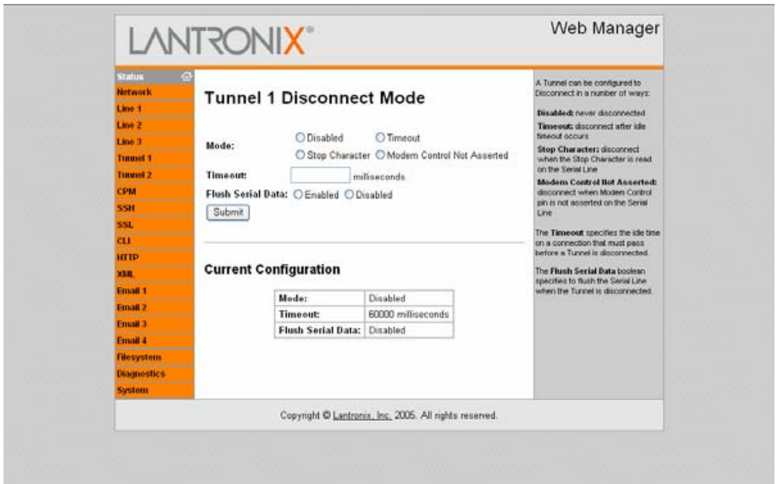
Disconnect Mode

Disconnect mode is disabled by default. When enabled, disconnect mode runs in the background of an active connection to determine when a disconnection is required.

To configure the tunnel's disconnect mode:

1. Click **Tunnel 1 → Disconnect Mode** from the navigation menu. The Tunnel 1 Disconnect Mode window displays.

Figure 4-17. Tunnel 1 Disconnect Mode



Tunnel 1 Disconnect Mode

Mode: ○ Disabled ○ Timeout ○ Stop Character ○ Modem Control Not Asserted

Timeout: milliseconds

Flush Serial Data: ○ Enabled ○ Disabled

Current Configuration

Mode:	Disabled
Timeout:	60000 milliseconds
Flush Serial Data:	Disabled

A Tunnel can be configured to Disconnect in a number of ways:

Disabled: never disconnected

Timeout: disconnect after idle timeout occurs

Stop Character: disconnect when the Stop Character is read on the Serial Line

Modem Control Not Asserted: disconnect when Modem Control pin is not asserted on the Serial Line

The **Timeout** specifies the idle time on a connection that must pass before a Tunnel is disconnected.

The **Flush Serial Data** boolean specifies to flush the Serial Line when the Tunnel is disconnected.

Copyright © Lantronix, Inc. 2005. All rights reserved.

2. Enter or modify the following fields:

Mode	Select **Disabled** to disable Disconnect Mode completely. Select **Timeout** to enable Disconnect Mode upon the timeout. Select **Stop Character** to enable Disconnect Mode upon receiving the stop character. Select **DSR Inactive** to enable Disconnect Mode if the Data Set Ready (DSR) pin is inactive on the serial line.
Timeout	Enter a time, in milliseconds, for the XPort AR to disconnect on a timeout (if specified as the **Mode**).
Flush Serial Data	Select **Enabled** to flush the serial data buffer on a disconnection.

3. Click **Submit**. Changes are applied immediately to the XPort AR.

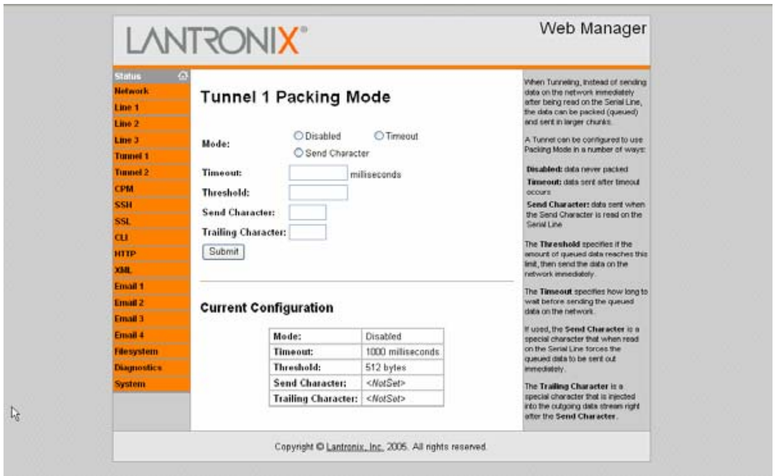
Packing Mode

When in packing mode, data is not transferred one byte at a time. Instead, data is queued and sent in segments.

To configure the tunnel's packing mode:

1. Select **Tunnel 1 → Packing Mode** from the navigation menu. The Tunnel 1 Packing Mode window displays.

Figure 4-18. Tunnel 1 Packing Mode



Tunnel 1 Packing Mode

Mode: ○ Disabled ○ Timeout ○ Send Character

Timeout: ______ milliseconds

Threshold: ______

Send Character: ______

Trailing Character: ______

Current Configuration

Mode:	Disabled
Timeout:	1000 milliseconds
Threshold:	512 bytes
Send Character:	<NotSet>
Trailing Character:	<NotSet>

When Tunneling, instead of sending data on the network immediately after being read on the Serial Line, the data can be packed (queued) and sent in larger chunks.

A Tunnel can be configured to use Packing Mode in a number of ways:

Disabled: data never packed

Timeout: data sent after timeout occurs

Send Character: data sent when the Send Character is read on the Serial Line

The **Threshold** specifies if the amount of queued data reaches this limit, then send the data on the network immediately.

The **Timeout** specifies how long to wait before sending the queued data on the network.

If used, the **Send Character** is a special character that when read on the Serial Line forces the queued data to be sent out immediately.

The **Trailing Character** is a special character that is injected into the outgoing data stream right after the **Send Character**.

Copyright © Lantronix, Inc. 2005. All rights reserved.

2. Enter or modify the following fields:

Mode	Select **Disabled** to disable Packing Mode completely. Select **Send Character** to send the queued data when the Send Character is received. Select **Timeout** to send data after the specified time has elapsed.
Timeout	Enter a time, in milliseconds, for the XPort AR to send the queued data.
Threshold	Send the queued data when the number of queued bytes reaches the **threshold**.
Send Character	Enter the **send character**. Upon receiving this character, the XPort AR sends out the queued data.
Trailing Character	Enter the **trailing character**. This character is sent immediately following the **send character**.

3. Click **Submit**. Changes are applied immediately to the XPort AR.

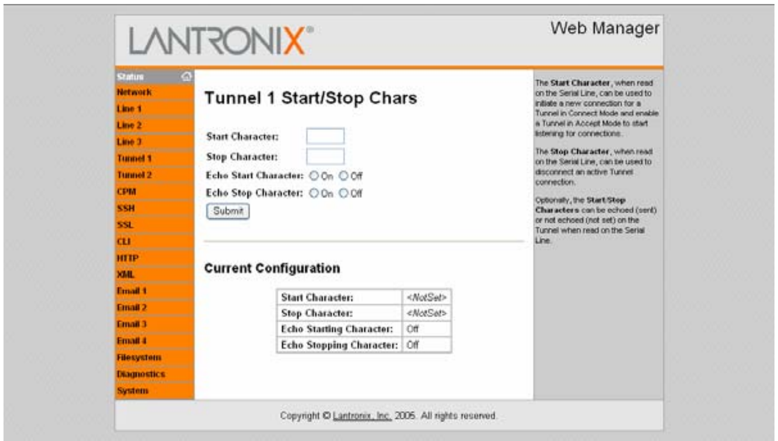
Start and Stop Characters

The XPort AR can be configured to start a tunnel when it receives a specific start character from the serial port. The XPort AR can also be configured to disconnect upon receiving the stop character.

To configure the start and stop characters mode:

1. Select **Tunnel 1 → Stop/Start Chars** from the navigation menu. The Tunnel 1 Start/Stop Chars window displays.

Figure 4-19. Tunnel 1 Start/Stop Chars



Tunnel 1 Start/Stop Chars

Start Character:

Stop Character:

Echo Start Character: ○ On ○ Off

Echo Stop Character: ○ On ○ Off

Current Configuration

Start Character:	<NotSet>
Stop Character:	<NotSet>
Echo Starting Character:	Off
Echo Stopping Character:	Off

The **Start Character**, when read on the Serial Line, can be used to initiate a new connection for a Tunnel in Connect Mode and enable a Tunnel in Accept Mode to start listening for connections.

The **Stop Character**, when read on the Serial Line, can be used to disconnect an active Tunnel connection.

Optionally, the **Start/Stop Characters** can be echoed (sent) or not echoed (not set) on the Tunnel when read on the Serial Line.

Copyright © Lantronix, Inc. 2005. All rights reserved.

2. Enter or modify the following fields:

Start Character	Enter the start character in either ASCII or hexadecimal notation.
Stop Character	Enter the start character in either ASCII or hexadecimal notation.
Echo Start Character	Select **On** to forward (tunnel) the start character.
Echo Stop Character	Select **On** to forward (tunnel) the stop character.

3. Click **Submit**. Changes are applied immediately to the XPort AR.

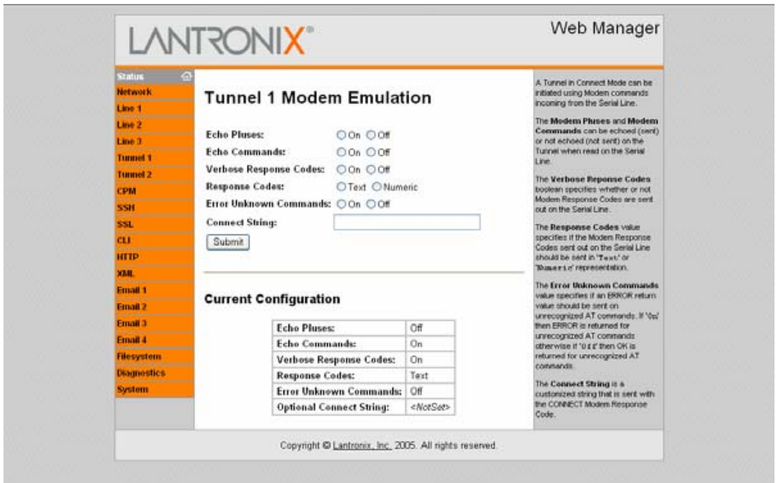
Modem Emulation

Configure the modem emulation settings when selecting Modem Emulation as the Tunnel 1 or Tunnel 2 Connect Mode type.

To configure modem emulation:

1. Select **Tunnel 1 → Modem Emulation** from the navigation menu. The Tunnel 1 Modem Emulation window displays.

Figure 4-20. Tunnel 1 Modem Emulation



Tunnel 1 Modem Emulation

Echo Pluses: ○ On ○ Off

Echo Commands: ○ On ○ Off

Verbose Response Codes: ○ On ○ Off

Response Codes: ○ Text ○ Numeric

Error Unknown Commands: ○ On ○ Off

Connect String:

Current Configuration

Echo Pluses:	Off
Echo Commands:	On
Verbose Response Codes:	On
Response Codes:	Text
Error Unknown Commands:	Off
Optional Connect String:	<NotSet>

A Tunnel in Connect Mode can be initiated using Modem commands incoming from the Serial Line.

The **Modem Pluses** and **Modem Commands** can be echoed (sent) or not echoed (not sent) on the Tunnel when read on the Serial Line.

The **Verbose Reponse Codes** boolean specifies whether or not Modem Response Codes are sent out on the Serial Line.

The **Response Codes** value specifies if the Modem Response Codes sent out on the Serial Line should be sent in 'Text' or 'Numeric' representation.

The **Error Unknown Commands** value specifies if an ERROR return value should be sent on unrecognized AT commands. If 'On' then ERROR is returned for unrecognized AT commands otherwise if 'Off' then OK is returned for unrecognized AT commands.

The **Connect String** is a customized string that is sent with the CONNECT Modem Response Code.

Copyright © Lantronix, Inc. 2005. All rights reserved.

2. Enter or modify the following fields:

Echo Pluses	Select **On** to echo "+++" when entering modem command mode
Echo Commands	Select **On** to echo the modem commands to the console.
Verbose Response Codes	Select **On** to send modem response codes out on the serial line.
Response Codes	Select the type of response code from either **Text** or **Numeric**.
Connect String	Enter the **connect string**. This modem initialization string prepares the modem for communications. It is a customized string sent with the "CONNECT" modem response code.

3. Click **Submit**. Changes are applied immediately to the XPort AR.

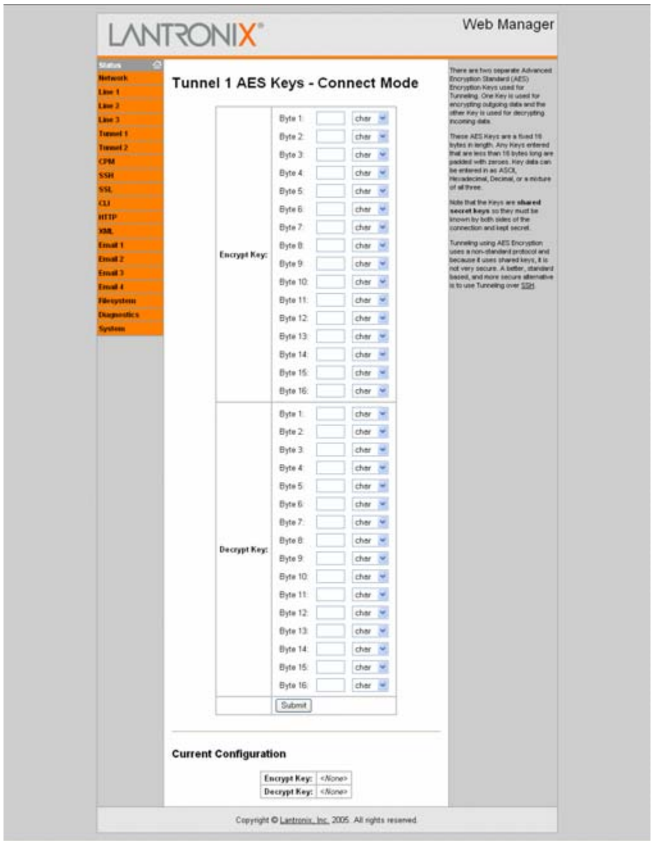
AES Keys – Connect Mode

Advanced Encryption Standard (AES) is an encryption algorithm for securing sensitive information by government agencies.

To configure the AES keys for connect mode:

1. Click **Tunnel 1→ AES Keys – Connect** from the navigation menu. The Tunnel 1 AES Keys – Connect window displays.

Figure 4-21. AES Keys – Connect



Tunnel 1 AES Keys - Connect Mode

There are two separate Advanced Encryption Standard (AES) Encryption Keys used for Tunneling. One Key is used for encrypting outgoing data and the other Key is used for decrypting incoming data.

These AES Keys are a fixed 16 bytes in length. Any Keys entered that are less than 16 bytes long are padded with zeroes. Key data can be entered in as ASCII, Hexadecimal, Decimal, or a mixture of all three.

Note that the Keys are **shared secret keys** so they must be known by both sides of the connection and kept secret.

Tunneling using AES Encryption uses a non-standard protocol and because it uses shared keys, it is not very secure. A better, standard based, and more secure alternative is to use Tunneling over SSH.

Current Configuration

Encrypt Key:	<None>
Decrypt Key:	<None>

Copyright © Lantronix, Inc. 2005. All rights reserved.

2. Enter or modify the following fields:

Encrypt Key	Enter the value for each byte. From the pull-down menu, select the format for the byte as either character, hexadecimal, or decimal notation. **Note:** *Any empty trailing bites that are not specified are set to 0.*
Decrypt Key	Enter the value for each byte of the decrypt key. From the pull-down menu, select the format for the byte as either character, hexadecimal, or decimal notation. **Note:** *Any empty trailing bites that are not specified are set to 0.*

3. Click **Submit**. Changes are applied immediately to the XPort AR.

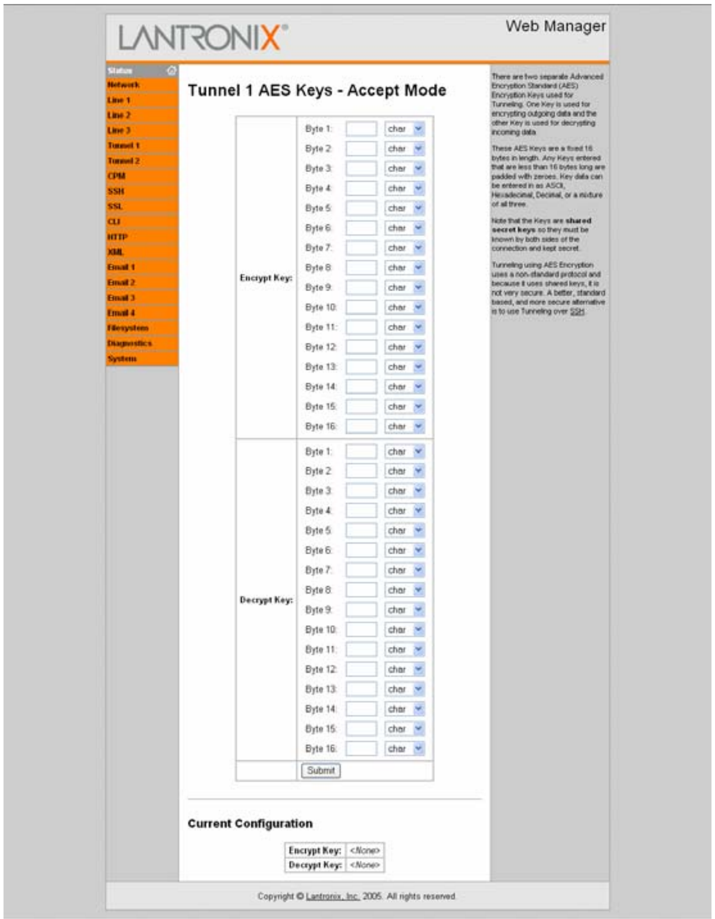
AES Keys – Accept Mode

Advanced Encryption Standard (AES) is an encryption algorithm for securing sensitive information by government agencies.

To configure the AES keys for accept mode:

1. Click **Tunnel 1 → AES Keys – Accept** from the navigation menu. The Tunnel 1 AES Keys – Accept window displays.

Figure 4-22. AES Keys – Accept



Tunnel 1 AES Keys - Accept Mode

Encrypt Key:	Byte 1:		char
	Byte 2:		char
	Byte 3:		char
	Byte 4:		char
	Byte 5:		char
	Byte 6:		char
	Byte 7:		char
	Byte 8:		char
	Byte 9:		char
	Byte 10:		char
	Byte 11:		char
	Byte 12:		char
	Byte 13:		char
	Byte 14:		char
	Byte 15:		char
	Byte 16:		char
Decrypt Key:	Byte 1:		char
	Byte 2:		char
	Byte 3:		char
	Byte 4:		char
	Byte 5:		char
	Byte 6:		char
	Byte 7:		char
	Byte 8:		char
	Byte 9:		char
	Byte 10:		char
	Byte 11:		char
	Byte 12:		char
	Byte 13:		char
	Byte 14:		char
	Byte 15:		char
	Byte 16:		char

There are two separate Advanced Encryption Standard (AES) Encryption Keys used for Tunneling. One Key is used for encrypting outgoing data and the other Key is used for decrypting incoming data.

These AES Keys are a fixed 16 bytes in length. Any Keys entered that are less than 16 bytes long are padded with zeroes. Key data can be entered in as ASCII, Hexadecimal, Decimal, or a mixture of all three.

Note that the Keys are **shared secret keys** so they must be known by both sides of the connection and kept secret.

Tunneling using AES Encryption uses a non-standard protocol and because it uses shared keys, it is not very secure. A better, standard based, and more secure alternative is to use Tunneling over SSH.

Current Configuration

Encrypt Key:	<None>
Decrypt Key:	<None>

Copyright © Lantronix, Inc. 2005. All rights reserved.

2. Enter or modify the following fields:

Encrypt Key	Enter the value for each byte. From the pull-down menu, select the format for the byte as either character, hexadecimal, or decimal notation. All trailing bytes not specified are set to 0.
Decrypt Key	Enter the value for each byte of the decrypt key. From the pull-down menu, select the format for the byte as either character, hexadecimal, or decimal notation. All trailing bytes not specified are set to 0.

3. Click **Submit**. Changes are applied immediately to the XPort AR.

Configurable Pin Manager

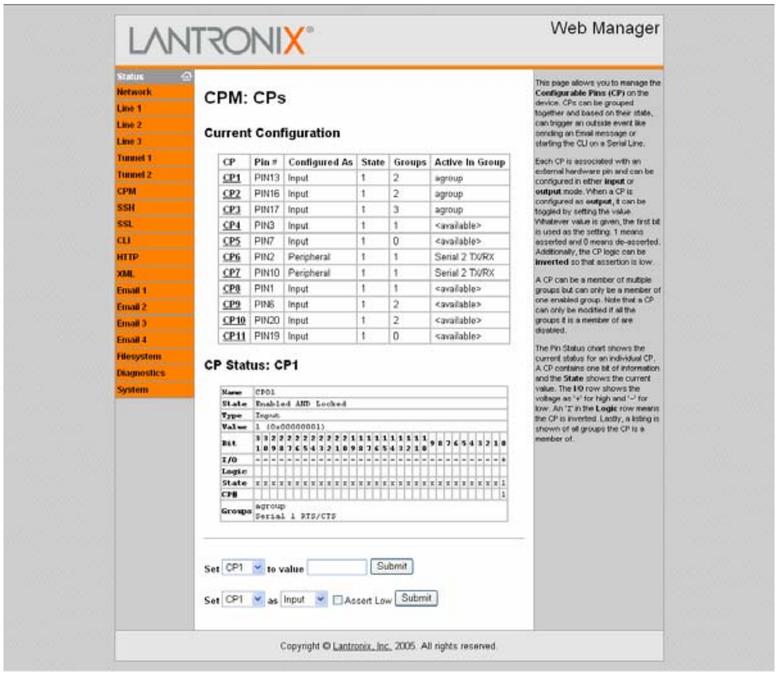
The XPort AR has 11 Configurable Pins (CPs). CPs can be grouped together using the Configurable Pin Manager (CPM). Each CP is associated to an external hardware pin. CPs can trigger an outside event (such as sending an email message or starting Command Mode).

CPM: Configurable Pins

To configure the XPort AR's CPs:

1. Click **CPM → CPs** from the navigation menu. The CPM: CPs window displays.

Figure 4-23. CPM: CPs



CPM: CPs

Current Configuration

CP	Pin #	Configured As	State	Groups	Active In Group
CP1	PIN13	Input	1	2	agroup
CP2	PIN16	Input	1	2	agroup
CP3	PIN17	Input	1	3	agroup
CP4	PIN3	Input	1	1	<available>
CP5	PIN7	Input	1	0	<available>
CP6	PIN2	Peripheral	1	1	Serial 2 TX/RX
CP7	PIN10	Peripheral	1	1	Serial 2 TX/RX
CP8	PIN1	Input	1	1	<available>
CP9	PIN6	Input	1	2	<available>
CP10	PIN20	Input	1	2	<available>
CP11	PIN19	Input	1	0	<available>

CP Status: CP1

Name	CP01																															
State	Enabled AND Locked																															
Type	Input																															
Value	1 (0x00000001)																															
Bit	31	30	29	28	27	26	25	24	23	22	21	20	19	18	17	16	15	14	13	12	11	10	9	8	7	6	5	4	3	2	1	0
I/O	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	+
Logic																																
State	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	1
CP#																																1
Groups	agroup Serial 1 RTS/CTS																															

Set CP1 to value [ ] Submit

Set CP1 as Input □ Assert Low Submit

This page allows you to manage the **Configurable Pins (CP)** on the device. CPs can be grouped together and based on their state, can trigger an outside event like sending an Email message or starting the CLI on a Serial Line.

Each CP is associated with an external hardware pin and can be configured in either **input** or **output** mode. When a CP is configured as **output**, it can be toggled by setting the value. Whatever value is given, the first bit is used as the setting. 1 means asserted and 0 means de-asserted. Additionally, the CP logic can be **inverted** so that assertion is low.

A CP can be a member of multiple groups but can only be a member of one enabled group. Note that a CP can only be modified if all the groups it is a member of are disabled.

The Pin Status chart shows the current status for an individual CP. A CP contains one bit of information and the **State** shows the current value. The **I/O** row shows the voltage as '+' for high and '-' for low. An 'I' in the **Logic** row means the CP is inverted. Lastly, a listing is shown of all groups the CP is a member of.

Copyright © Lantronix, Inc. 2005. All rights reserved.

2. The Current Configuration table displays the current settings for each CP:

Current Configuration

CP	Indicates the Configurable Pin number.
Pin #	Indicates the hardware pin number associated with the CP.
Configured As	Displays the CPs configuration. A CP configured as **Input** is set to read input. A CP configured as **Output** drives data out of the XPort AR. **Peripheral** is a setting assigned by the XPort AR.
State	A value of **1** means asserted. **0** means de-asserted. **I** indicates the CP is inverted.
Groups	Indicates the number of groups in which the CP is a member.
Active In Group	A CP can be a member of several groups. However, it may only be active in one group. This field displays the group in which the CP is active.

3. To display the CP status of a specific pin, click the CP number under the Current Configuration table. The CP Status table displays detailed information about the CP.

CP Status

Name	Displays the CP number.
State	Current enable state of the CP. ***Note:*** *Peripheral pins are locked.*
Value	Displays the last bit in the CP's current value.
Bit	Visual display of the 32 bit placeholders for a CP.
I/O	A "+" symbol indicates the CP is asserted (the voltage is high). A "-" indicates the CP voltage is low.
Logic	An "I" indicates the CP is inverted.
State	Displays the assertion value of the corresponding bit.
CP#	Displays the CP number.
Groups	Lists the groups in which the CP is a member.

4. To change a CP's value:

   a) Select the CP from the drop-down list.

   b) Enter the CP's value.

   c) Click **Submit**. Changes are applied immediately to the XPort AR.

5. To change a CP's configuration:

   a) Select the CP from the drop-down list.

   b) Select the CP's configuration from the drop-down list.

   c) (If necessary) Select **the Assert Low** checkbox.

   d) Click **Submit**. Changes are applied immediately to the XPort AR.

Note: *To modify a CP, all groups in which it is a member must be disabled.*

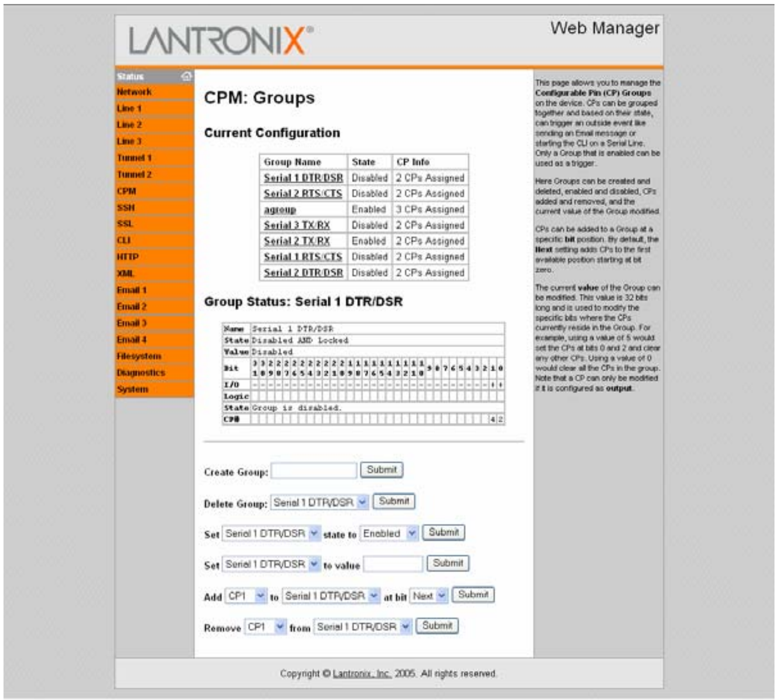
CPM: Groups

The CP Groups page allows for the management of CP groups. Create a CP group and add CPs to it. A group, based on its state, triggers outside events (such as sending email messages). Only an enabled group can be used as a trigger.

To configure the XPort AR's CP groups:

1. Click **CPM → Groups** from the navigation menu. The CPM: Groups window displays.

Figure 4-24. CPM: Groups



CPM: Groups

Current Configuration

Group Name	State	CP Info
Serial 1 DTR/DSR	Disabled	2 CPs Assigned
Serial 2 RTS/CTS	Disabled	2 CPs Assigned
agroup	Enabled	3 CPs Assigned
Serial 3 TX/RX	Disabled	2 CPs Assigned
Serial 2 TX/RX	Enabled	2 CPs Assigned
Serial 1 RTS/CTS	Disabled	2 CPs Assigned
Serial 2 DTR/DSR	Disabled	2 CPs Assigned

Group Status: Serial 1 DTR/DSR

Name	Serial 1 DTR/DSR																															
State	Disabled AND Locked																															
Value	Disabled																															
Bit	31	30	29	28	27	26	25	24	23	22	21	20	19	18	17	16	15	14	13	12	11	10	9	8	7	6	5	4	3	2	1	0
I/O	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	I	I
Logic																																
State	Group is disabled.																															
CP#																															4	2

Create Group: [ ] Submit

Delete Group: Serial 1 DTR/DSR Submit

Set Serial 1 DTR/DSR state to Enabled Submit

Set Serial 1 DTR/DSR to value [ ] Submit

Add CP1 to Serial 1 DTR/DSR at bit Next Submit

Remove CP1 from Serial 1 DTR/DSR Submit

This page allows you to manage the **Configurable Pin (CP) Groups** on the device. CPs can be grouped together and based on their state, can trigger an outside event like sending an Email message or starting the CLI on a Serial Line. Only a Group that is enabled can be used as a trigger.

Here Groups can be created and deleted, enabled and disabled, CPs added and removed, and the current value of the Group modified.

CPs can be added to a Group at a specific **bit** position. By default, the **Next** setting adds CPs to the first available position starting at bit zero.

The current **value** of the Group can be modified. This value is 32 bits long and is used to modify the specific bits where the CPs currently reside in the Group. For example, using a value of 5 would set the CPs at bits 0 and 2 and clear any other CPs. Using a value of 0 would clear all the CPs in the group. Note that a CP can only be modified if it is configured as **output**.

Copyright © Lantronix, Inc. 2005. All rights reserved.

2. The Current Configuration table displays the current settings for each CP group:

Current Configuration

Group Name	Displays the CP group's name.
State	Indicates whether the group is enabled or disabled.
CP Info	Provides CP group information.

3. To display the status of a specific group, click the CP group name under the Current Configuration table. The Group Status table displays, providing detailed information about the CP group.

Group Status

Name	Displays the CP Group name.
State	Current enable state of the CP group. ***Note:*** *Peripheral pins are locked.*

Value	Displays the CP group's current value.
Bit	Visual display of the 32 bit placeholders for a CP.
I/O	A "+" symbol indicates the CP's bit position is asserted (the voltage is high). A "-" indicates the CP voltage is low.
Logic	An "I" indicates the CP is inverted.
State	Displays the assertion value of the corresponding bit.
CP#	Displays the Configurable Pin number and its bit position in the CP group.

2. To create a CP group:

   a) Enter a group name in the **Create Group** field.

   b) Click **Submit**. Changes are applied immediately to the XPort AR.

3. To delete a CP group:

   a) Select the CP group from the **Delete Group** drop-down list.

   b) Click **Submit**. Changes are applied immediately to the XPort AR.

4. To enable or disable a CP group:

   a) Select the CP group from the **Set** drop-down list.

   b) Select the state (**Enabled** or **Disabled**) from the drop-down list.

   c) Click **Submit**. Changes are applied immediately to the XPort AR.

5. To set a CP group's value:

   a) Select the CP group from the **Set** drop-down list.

   b) Enter the CP group's value in the **value** field.

   c) Click **Submit**. Changes are applied immediately to the XPort AR.

6. To add CP to a CP group:

   a) Select the CP from the **Add** drop-down list.

   b) Select the CP group from the drop-down list.

   c) Select the CP's bit location from the **bit** drop-down menu.

   d) Click **Submit**. Changes are applied immediately to the XPort AR.

7. To delete a CP from a CP group:

   a) Select the CP from the **Remove** drop-down list.

   b) Select the CP group from the drop-down list.

   c) Click **Submit**. Changes are applied immediately to the XPort AR.

SSH Settings

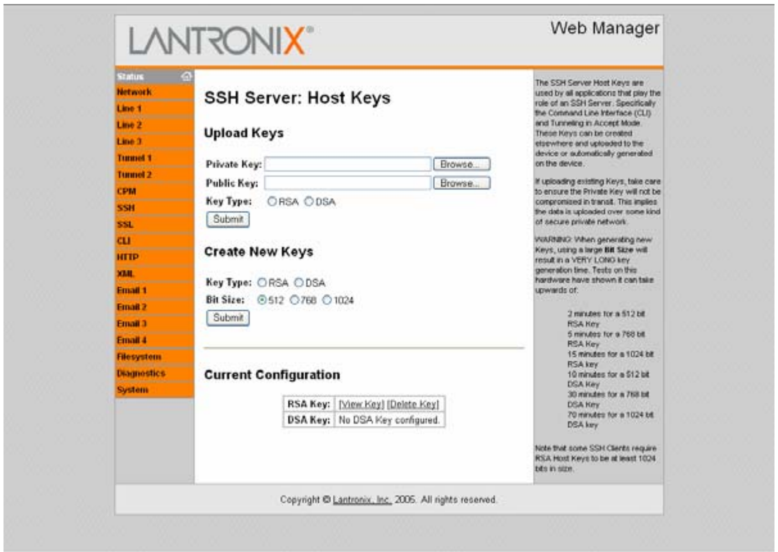
Secure Shell (SSH) is a protocol used to access a remote computer over an encrypted channel. It is a protocol for managing the security of data transmission over the Internet. It provides encryption, authentication, and message integrity services. Select the **SSH** link on the left menu bar to display the **SSH** menu over an encrypted channel. The sub-menus allow for the configuration of the SSH server (when the XPort AR acts as the server) and the SSH client (when the XPort AR acts as the client).

SSH Server’s Host Keys

To configure the SSH server’s host keys:

1. Click **SSH → Server Host Keys** from the navigation menu. The SSH Server: Host Keys window displays.

Figure 4-25. SSH Server: Host Keys



SSH Server: Host Keys

Upload Keys

Private Key: Browse...
Public Key: Browse...
Key Type: ○RSA ○DSA
Submit

Create New Keys

Key Type: ○RSA ○DSA
Bit Size: ●512 ○768 ○1024
Submit

Current Configuration

RSA Key:	[View Key] [Delete Key]
DSA Key:	No DSA Key configured.

The SSH Server Host Keys are used by all applications that play the role of an SSH Server. Specifically the Command Line Interface (CLI) and Tunneling in Accept Mode. These Keys can be created elsewhere and uploaded to the device or automatically generated on the device.

If uploading existing Keys, take care to ensure the Private Key will not be compromised in transit. This implies the data is uploaded over some kind of secure private network.

WARNING: When generating new Keys, using a large **Bit Size** will result in a VERY LONG key generation time. Tests on this hardware have shown it can take upwards of:

2 minutes for a 512 bit RSA Key
5 minutes for a 768 bit RSA Key
15 minutes for a 1024 bit RSA key
10 minutes for a 512 bit DSA Key
30 minutes for a 768 bit DSA Key
70 minutes for a 1024 bit DSA key

Note that some SSH Clients require RSA Host Keys to be at least 1024 bits in size.

Copyright © Lantronix, Inc. 2005. All rights reserved.

2. Enter or modify the following fields:

Host Keys

Private Key	Browse and locate the private key. Required when the **Public Key** is specified.
Public Key	Browse and locate the public key. Required when the **Private Key** is specified
Key Type	Select the key type. **DSA** is more secure than **RSA**. *__Note:__ One set of RSA keys and one set of DSA keys are accepted.*

3. Click **Submit**. Changes are applied immediately to the XPort AR.

4. To create new keys, select the following option buttons:

Create New Keys

Key Type	Select **RSA** or **DSA**.
Bit Size	Select the size of the key. Large bit keys require more time to generate. *Note: Certain SSH clients require RSA host keys to be at least 1024 bits.*

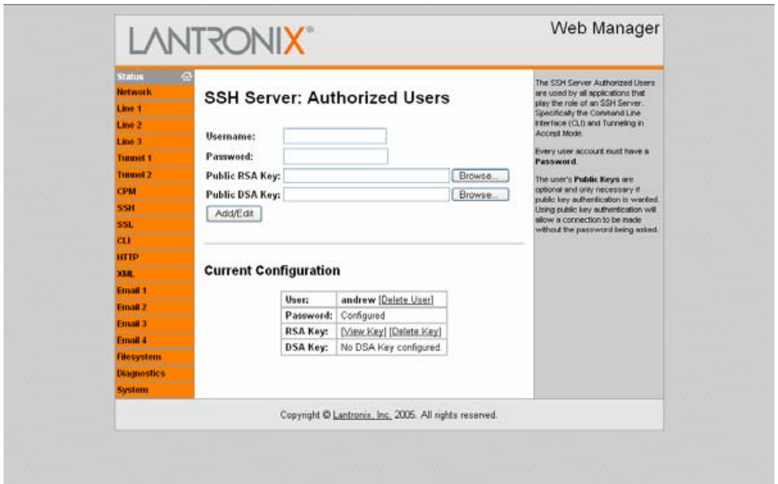
5. Click **Submit**. Changes are applied immediately to the XPort AR.

SSH Server's Authorized Users

To configure the SSH server's authorized users:

1. Click **SSH → Server Authorized Users** from the navigation menu. The SSH Server: Authorized Users window displays.

Figure 4-26. SSH Server: Authorized Users



SSH Server: Authorized Users

Username:

Password:

Public RSA Key:

Public DSA Key:

Current Configuration

User:	andrew [Delete User]
Password:	Configured
RSA Key:	[View Key] [Delete Key]
DSA Key:	No DSA Key configured

The SSH Server Authorized Users are used by all applications that play the role of an SSH Server. Specifically the Command Line Interface (CLI) and Tunneling in Accept Mode.

Every user account must have a **Password**.

The user's **Public Keys** are optional and only necessary if public key authentication is wanted. Using public key authentication will allow a connection to be made without the password being asked.

Copyright © Lantronix, Inc. 2005. All rights reserved.

2. Enter or modify the following fields:

Authorized Users

Username	Enter the username for an authorized user. Required when the **Password** is specified.
Password	Enter the password for SSH login to the XPort AR. Required when the **Username** is specified.
Public RSA Key	Browse and locate the RSA public key for this authorized user. This is used for key authentication. When successful, no password is requested.
Public DSA Key	Browse and locate the DSA public key for this authorized user. This is used for key authentication. When successful, no password is requested.

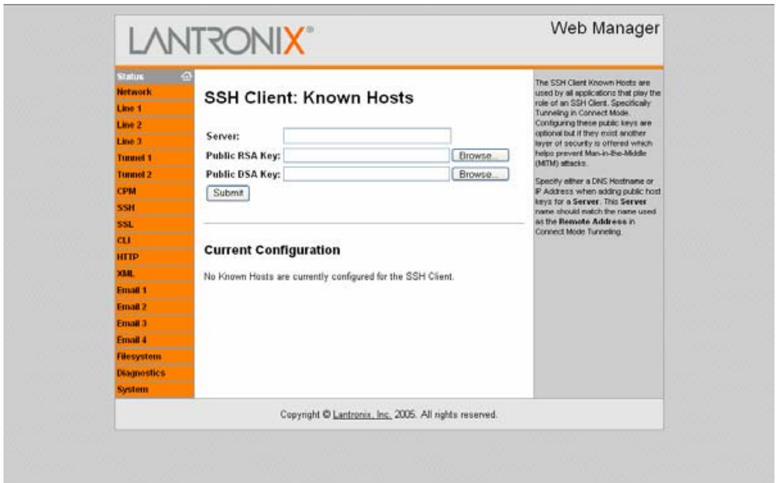
3. Click **Submit**. Changes are applied immediately to the XPort AR.

SSH Client Known Hosts

To configure the SSH client's known hosts:

1. Click **SSH → Client Known Hosts** from the navigation menu. The SSH Client: Known Hosts window displays.

Figure 4-27. SSH Client: Known Hosts



SSH Client: Known Hosts

Server:

Public RSA Key:

Public DSA Key:

Current Configuration

No Known Hosts are currently configured for the SSH Client.

The SSH Client Known Hosts are used by all applications that play the role of an SSH Client. Specifically Tunneling in Connect Mode. Configuring these public keys are optional but if they exist another layer of security is offered which helps prevent Man-in-the-Middle (MITM) attacks.

Specify either a DNS Hostname or IP Address when adding public host keys for a **Server**. This **Server** name should match the name used as the **Remote Address** in Connect Mode Tunneling.

Copyright © Lantronix, Inc. 2005. All rights reserved.

2. Enter or modify the following fields:

Server	Enter the hostname or IP address of the remote server location.
Public RSA Key	Click **Browse** to locate the public RSA key to use when authenticating the connection to the server.
Public DSA Key	Click **Browse** to locate the public DSA key to use when authenticating the connection to the server.

Note: *These fields are not required for communication. They protect against Man-In-The-Middle (MITM) attacks.*

3. In the **Current Configuration** table, delete currently stored fields as necessary.

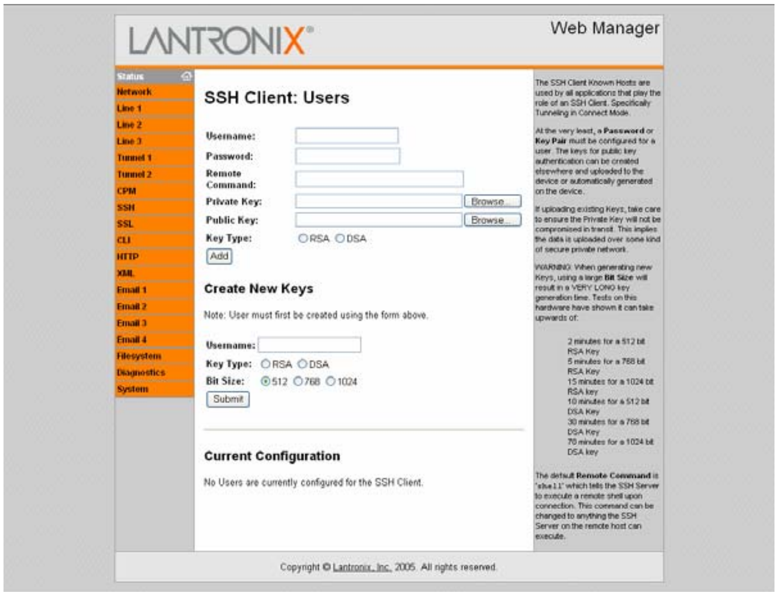
4. Click **Submit**. Changes are applied immediately to the XPort AR.

SSH Client User Configuration

To configure the SSH client's users:

1. Click **SSH → SSH Client Users** from the navigation menu. The SSH Client: Users window displays.

Figure 4-28. SSH Client: Users



SSH Client: Users

Username:

Password:

Remote Command:

Private Key:

Public Key:

Key Type: ○ RSA ○ DSA

Create New Keys

Note: User must first be created using the form above.

Username:

Key Type: ○ RSA ○ DSA

Bit Size: ● 512 ○ 768 ○ 1024

Current Configuration

No Users are currently configured for the SSH Client.

The SSH Client Known Hosts are used by all applications that play the role of an SSH Client. Specifically Tunneling in Connect Mode.

At the very least, a **Password** or **Key Pair** must be configured for a user. The keys for public key authentication can be created elsewhere and uploaded to the device or automatically generated on the device.

If uploading existing Keys, take care to ensure the Private Key will not be compromised in transit. This implies the data is uploaded over some kind of secure private network.

WARNING: When generating new Keys, using a large **Bit Size** will result in a VERY LONG key generation time. Tests on this hardware have shown it can take upwards of:

2 minutes for a 512 bit RSA Key
5 minutes for a 768 bit RSA Key
15 minutes for a 1024 bit RSA key
10 minutes for a 512 bit DSA Key
30 minutes for a 768 bit DSA Key
70 minutes for a 1024 bit DSA key

The default **Remote Command** is "shell1" which tells the SSH Server to execute a remote shell upon connection. This command can be changed to anything the SSH Server on the remote host can execute.

Copyright © Lantronix, Inc. 2005. All rights reserved.

2. Enter or modify the following fields:

Username	Enter the XPort AR's username for use when connecting to the server.
Password	Enter the password associated with the username.
Remote Command	Enter the remote command to provide to the server. This command triggers the desired or appropriate application to execute. A shell starts by default.
Private Key	Browse and locate the private key to use for authentication with the remote server.
Public Key	Browse and locate the public key to use for authentication with the remote server.
Key Type	Select the key type. **DSA** is more secure than **RSA**.

3. To create new keys, select the following option buttons:

Create New Keys

Key Type	Select **RSA** or **DSA**.
Bit Size	Select the size of the key. ***Note:*** *Large bit keys require more time to generate.*

4. Click **Submit**. Changes are applied immediately to the XPort AR.

5. In the **Current Configuration** table, delete currently stored fields as necessary.

6. Click **Submit**. Changes are applied immediately to the XPort AR.

SSL Settings

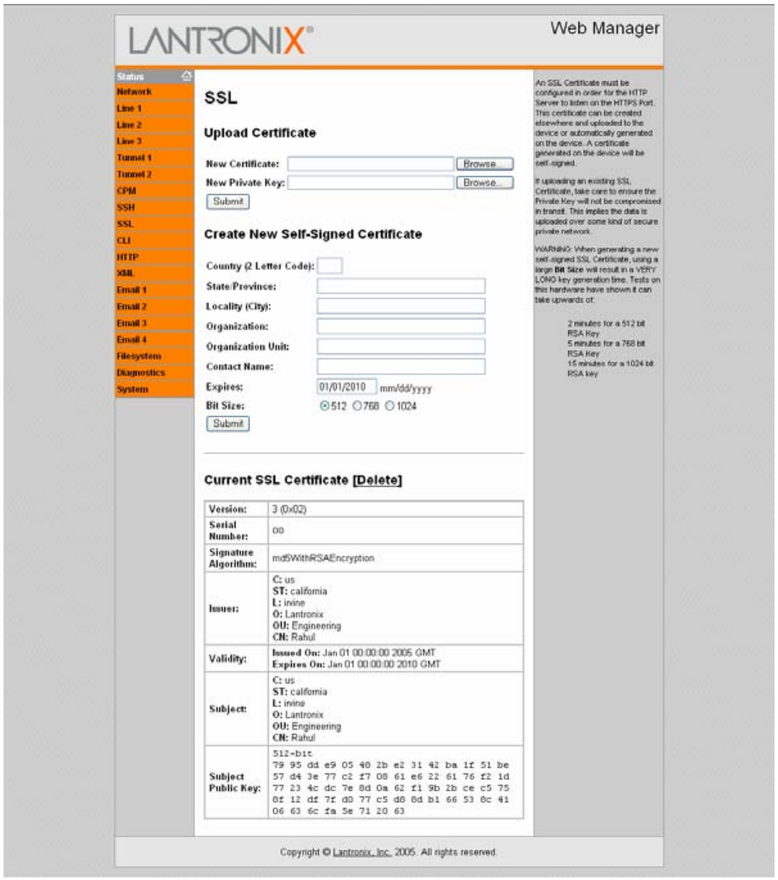
Secure Socket Layer (SSL) is a protocol for managing the security of data transmission over the Internet. It provides encryption, authentication, and message integrity services. SSL is widely used for secure communication to a web server.

Select the **SSL** link on the left menu bar to display the **SSL** menu. The Web Manager also permits the creation of self-signed certificates. This type of SSL certificate is a certificate not signed by a valid Certificate Authority (CA).

To configure the XPort AR's SSL settings:

1. Click **SSL** from the main menu. The SSL window displays.

Figure 4-29. SSL



SSL

Upload Certificate

New Certificate:

New Private Key:

Create New Self-Signed Certificate

Country (2 Letter Code):

State/Province:

Locality (City):

Organization:

Organization Unit:

Contact Name:

Expires: 01/01/2010 mm/dd/yyyy

Bit Size: ● 512 ○ 768 ○ 1024

Current SSL Certificate [Delete]

Version:	3 (0x02)
Serial Number:	00
Signature Algorithm:	md5WithRSAEncryption
Issuer:	**C:** us **ST:** california **L:** irvine **O:** Lantronix **OU:** Engineering **CN:** Rahul
Validity:	**Issued On:** Jan 01 00:00:00 2005 GMT **Expires On:** Jan 01 00:00:00 2010 GMT
Subject:	**C:** us **ST:** california **L:** irvine **O:** Lantronix **OU:** Engineering **CN:** Rahul
Subject Public Key:	512-bit 79 95 dd e9 05 40 2b e2 31 42 ba 1f 51 be 57 d4 3e 77 c2 f7 08 61 e6 22 61 76 f2 1d 77 23 4c dc 7e 8d 0a 62 f1 9b 2b ce c5 75 0f 12 df 7f d0 77 c5 d8 0d b1 66 53 0c 41 06 63 6c fa 5e 71 20 63

An SSL Certificate must be configured in order for the HTTP Server to listen on the HTTPS Port. This certificate can be created elsewhere and uploaded to the device or automatically generated on the device. A certificate generated on the device will be self-signed.

If uploading an existing SSL Certificate, take care to ensure the Private Key will not be compromised in transit. This implies the data is uploaded over some kind of secure private network.

WARNING: When generating a new self-signed SSL Certificate, using a large **Bit Size** will result in a VERY LONG key generation time. Tests on this hardware have shown it can take upwards of:

2 minutes for a 512 bit RSA Key
5 minutes for a 768 bit RSA Key
15 minutes for a 1024 bit RSA key

Copyright © Lantronix, Inc. 2005. All rights reserved.

2. Enter or modify the following fields:

Upload Certificate

New Certificate	Browse and locate the digital certificate for use in SSL communications. Required field when configuring the **Private Key**.
Private Key	Browse and locate the private key. This private key is a secret and known only to the certificate's owner. Required field when configuring a **New Certificate**.

3. Click **Submit**. Changes are applied immediately to the XPort AR.

4. To create a new self-signed certificate, enter the following information:

Create New Self-Signed Certificate

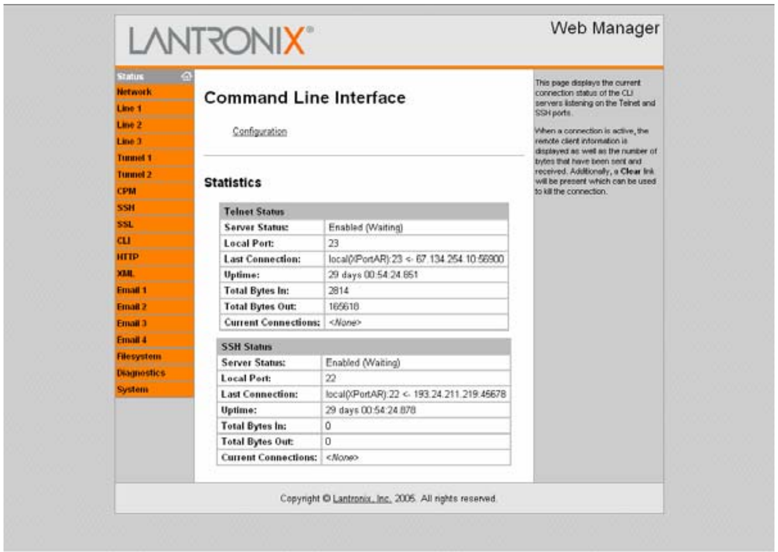
Country	Enter the 2-letter country code.
State/Province	Enter the state or province within the country.
Locality	Enter the city within the **State/Province**.
Organization	The name of the organization owning the certificate.
Organization Unit	The organization’s division (unit) using the certificate.
Contact Name	Enter the Contact Name for the certificate.
Expires	Enter, in mm/dd/yyy format, the certificate’s expiry date.
Bit Size	Select the certificate’s bit size. ***Note:*** *Large bit keys require more time to generate.*

5. Click **Submit**. Changes are applied immediately to the XPort AR.

Command Line Interface Settings

Select the **CLI** link on the left menu bar to display the **Command Line Interface** menu.

Figure 4-30. Command Line Interface Statistics



Command Line Interface

Statistics

Telnet Status	
Server Status:	Enabled (Waiting)
Local Port:	23
Last Connection:	local(XPortAR):23 <- 67.134.254.10:56900
Uptime:	29 days 00:54:24.851
Total Bytes In:	2814
Total Bytes Out:	165618
Current Connections:	*<None>*

SSH Status	
Server Status:	Enabled (Waiting)
Local Port:	22
Last Connection:	local(XPortAR):22 <- 193.24.211.219:45678
Uptime:	29 days 00:54:24.878
Total Bytes In:	0
Total Bytes Out:	0
Current Connections:	*<None>*

This page displays the current connection status of the CLI servers listening on the Telnet and SSH ports.

When a connection is active, the remote client information is displayed as well as the number of bytes that have been sent and received. Additionally, a **Clear** link will be present which can be used to kill the connection.

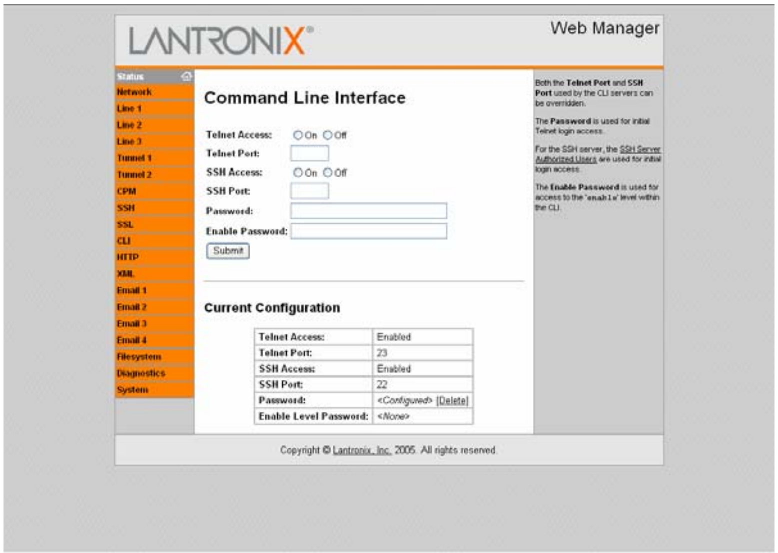
Copyright © Lantronix, Inc. 2006. All rights reserved.

CLI Configuration

To configure the CLI:

1. Click **CLI → Configuration** from the navigation menu. The Command Line Interface window displays.

Figure 4-31. Command Line Interface Configuration



Command Line Interface

Telnet Access: ○ On ○ Off
Telnet Port:
SSH Access: ○ On ○ Off
SSH Port:
Password:
Enable Password:

Current Configuration

Telnet Access:	Enabled
Telnet Port:	23
SSH Access:	Enabled
SSH Port:	22
Password:	*<Configured>* [Delete]
Enable Level Password:	*<None>*

Both the **Telnet Port** and **SSH Port** used by the CLI servers can be overridden.

The **Password** is used for initial Telnet login access.

For the SSH server, the SSH Server Authorized Users are used for initial login access.

The **Enable Password** is used for access to the "enable" level within the CLI.

Copyright © Lantronix, Inc. 2005. All rights reserved.

2. Enter or modify the following fields:

Telnet Access	Select **On** to enable Telnet access. Telnet is enabled by default.
Telnet Port	Enter the Telnet port to use for Telnet access. The default is 23.
SSH Access	Select **On** to enable SSH access. SSH is enabled by default.
SSH Port	Enter the SSH port to use for SSH access. The default is 22.
Password	Enter the password for Telnet access.
Enable Password	Enter the password for access to the Command Mode Enable level. There is no password by default.

3. Click **Submit**. Changes are applied immediately to the XPort AR.

HTTP Settings

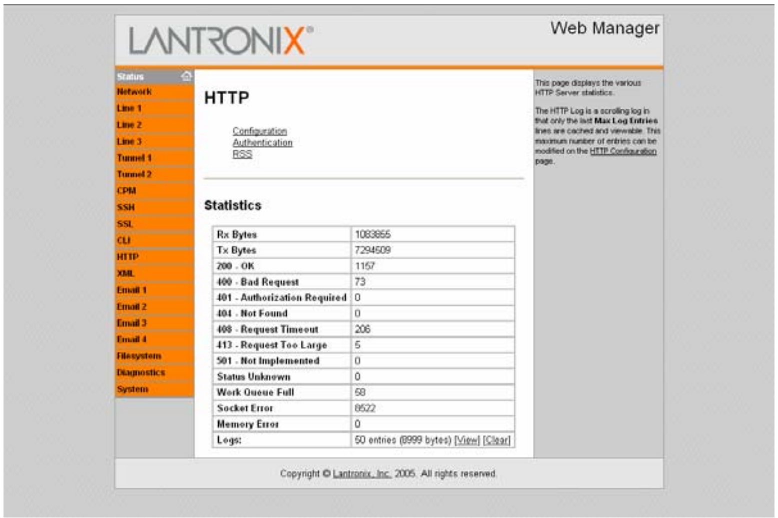
Hypertext Transfer Protocol (HTTP) is the transport protocol for communicating hypertext documents on the Internet. HTTP defines how messages are formatted and transmitted. It also defines the actions Web servers and browsers should take in response to different commands.

Select the **HTTP** link on the left menu bar to display the **HTTP** menu. The sub-menus allow for HTTP configuration, HTTP authentication administration, or RSS configuration.

To view HTTP statistics:

1. Click **HTTP → Statistics** from the navigation menu. The HTTP Statistics window displays.

Figure 4-32. HTTP Statistics



HTTP

Statistics

Rx Bytes	1083855
Tx Bytes	7294509
200 - OK	1157
400 - Bad Request	73
401 - Authorization Required	0
404 - Not Found	0
408 - Request Timeout	206
413 - Request Too Large	5
501 - Not Implemented	0
Status Unknown	0
Work Queue Full	58
Socket Error	8522
Memory Error	0
Logs:	50 entries (8999 bytes) [View] [Clear]

This page displays the various HTTP Server statistics.

The HTTP Log is a scrolling log in that only the last **Max Log Entries** lines are cached and viewable. This maximum number of entries can be modified on the HTTP Configuration page.

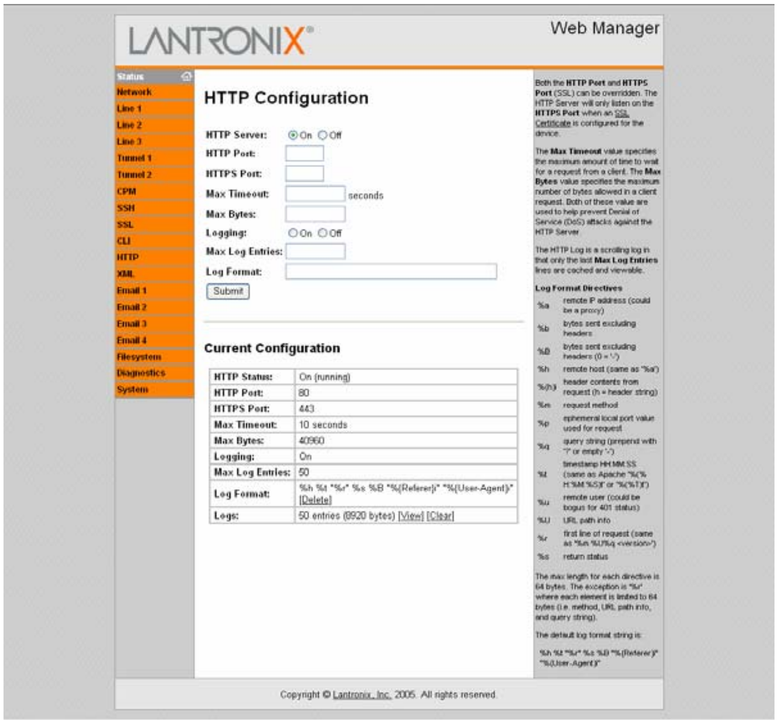
Copyright © Lantronix, Inc. 2005. All rights reserved.

HTTP Configuration

To configure HTTP:

1. Click **HTTP → HTTP Configuration** from the navigation menu. The HTTP Configuration window opens.

Figure 4-33. HTTP Configuration



HTTP Configuration

HTTP Server: ● On ○ Off
HTTP Port:
HTTPS Port:
Max Timeout: seconds
Max Bytes:
Logging: ○ On ○ Off
Max Log Entries:
Log Format:

Current Configuration

HTTP Status:	On (running)
HTTP Port:	80
HTTPS Port:	443
Max Timeout:	10 seconds
Max Bytes:	40960
Logging:	On
Max Log Entries:	50
Log Format:	%h %t "%r" %s %B "%{Referer}i" "%{User-Agent}i" [Delete]
Logs:	50 entries (8920 bytes) [View] [Clear]

Both the **HTTP Port** and **HTTPS Port** (SSL) can be overridden. The HTTP Server will only listen on the **HTTPS Port** when an SSL Certificate is configured for the device.

The **Max Timeout** value specifies the maximum amount of time to wait for a request from a client. The **Max Bytes** value specifies the maximum number of bytes allowed in a client request. Both of these value are used to help prevent Denial of Service (DoS) attacks against the HTTP Server.

The HTTP Log is a scrolling log in that only the last **Max Log Entries** lines are cached and viewable.

Log Format Directives

%a	remote IP address (could be a proxy)
%b	bytes sent excluding headers
%B	bytes sent excluding headers (0 = '-')
%h	remote host (same as "%a")
%{h}i	header contents from request (h = header string)
%m	request method
%p	ephemeral local port value used for request
%q	query string (prepend with '?' or empty '-')
%t	timestamp HH:MM:SS (same as Apache "%(%H:%M:%S)t" or "%(%T)t")
%u	remote user (could be bogus for 401 status)
%U	URL path info
%r	first line of request (same as "%m %U%q <version>")
%s	return status

The max length for each directive is 64 bytes. The exception is "%r" where each element is limited to 64 bytes (i.e. method, URL path info, and query string).

The default log format string is:

%h %t "%r" %s %B "%{Referer}i" "%{User-Agent}i"

Copyright © Lantronix, Inc. 2005. All rights reserved.

2. Enter or modify the following fields:

HTTP Server	Select **On** to enable the HTTP server.
HTTP Port	Enter the port for the HTTP server to use. The default is 80.
HTTPS Port	Enter the port for the HTTPS server to use. The default is 443. The HTTP server only listens on the **HTTPS Port** when an SSL certificate is configured.
Max Timeout	Enter the maximum time for the HTTP server to wait when receiving a request. This prevents Denial-of-Service (DoS) attacks. The default is 10 seconds.
Max Bytes	Enter the maximum number of bytes the HTTP server accepts when receiving a request. The default is 32 KB (this prevents DoS attacks).
Logging	Select **On** to enable HTTP server logging.
Max Log Entries	Sets the maximum number of HTTP server log entries. Only the last **Max Log Entries** are cached and viewable.
Log Format	Set the log format string for the HTTP server. The **Log Format** directives are as follows: **%a** - remote IP address (could be a proxy) **%b** - bytes sent excluding headers **%B** - bytes sent excluding headers (0 = '-') **%h** - remote host (same as '%a') **%{h}i** - header contents from request (h = header string) **%m** - request method **%p** - ephemeral local port value used for request **%q** - query string (prepend with '?' or empty '-') **%t** - timestamp HH:MM:SS (same as Apache '%(%H:%M:%S)t' or '%(%T)t') **%u** - remote user (could be bogus for 401 status) **%U** - URL path info **%r** - first line of request (same as '%m %U%q <version>') **%s** - return status

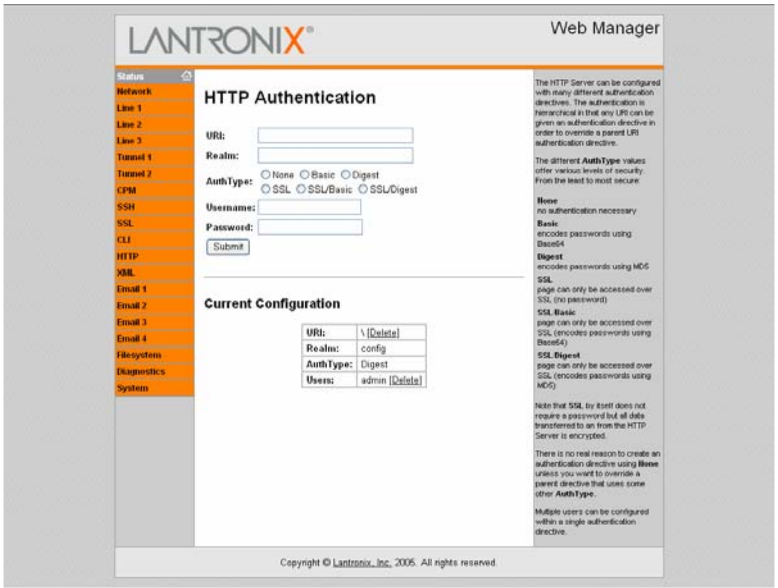
2. Click **Submit**. Changes are applied immediately to the XPort AR.

HTTP Authentication

To configure HTTP authentication settings:

1. Click **HTTP → Authentication** from the navigation menu. The HTTP Authentication window opens.

Figure 4-34. HTTP Authentication



HTTP Authentication

URI:

Realm:

AuthType: ○ None ○ Basic ○ Digest ○ SSL ○ SSL/Basic ○ SSL/Digest

Username:

Password:

Current Configuration

URI:	\ [Delete]
Realm:	config
AuthType:	Digest
Users:	admin [Delete]

The HTTP Server can be configured with many different authentication directives. The authentication is hierarchical in that any URI can be given an authentication directive in order to override a parent URI authentication directive.

The different **AuthType** values offer various levels of security. From the least to most secure:

None
no authentication necessary

Basic
encodes passwords using Base64

Digest
encodes passwords using MD5

SSL
page can only be accessed over SSL (no password)

SSL Basic
page can only be accessed over SSL (encodes passwords using Base64)

SSL Digest
page can only be accessed over SSL (encodes passwords using MD5)

Note that **SSL** by itself does not require a password but all data transferred to an from the HTTP Server is encrypted.

There is no real reason to create an authentication directive using **None** unless you want to override a parent directive that uses some other **AuthType**.

Multiple users can be configured within a single authentication directive.

Copyright © Lantronix, Inc. 2005. All rights reserved.

2. Enter or modify the following fields:

URI	Enter the Uniform Resource Identifier (URI).
Realm	Enter the domain, or realm, used for HTTP. Required with the **URI** field.
Auth Type	Select the authentication type. **None** means no authentication is necessary. **Basic** encodes passwords using Base64. **Digest** encodes passwords using MD5. **SSL** means the page can only be accessed over SSL (no password is required). **SSL/Basic** means the page is accessible only over SSL and encodes passwords using Base64. **SSL/Digest** means the page is accessible only over SSL and encodes passwords using MD5.
Username	Enter the **Username** used to access the **URI**.
Password	Enter the **Password** for the **Username**.

3. In the **Current Configuration** table, delete and clear currently stored fields as necessary.

4. Click **Submit**. Changes are applied immediately to the XPort AR.

Note: *More than one **Username** per **URI** is permitted. Click **Submit** and enter the next **Username** as necessary.*

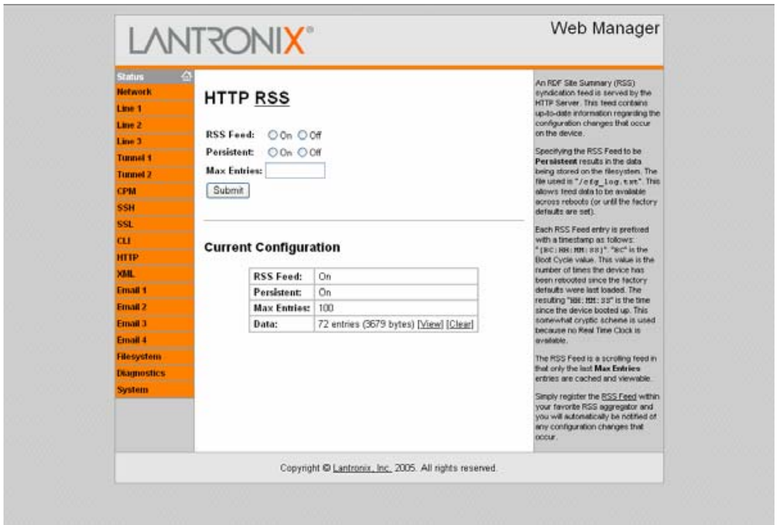
HTTP RSS

Rich Site Summary (RSS) is a method of feeding online content to Web users. Instead of actively searching for XPort AR configuration changes, RSS feeds permit viewing only relevant and new information regarding changes made to the XPort AR via an RSS publisher. The RSS feeds are also stored to the filesystem's cfg_log.txt file.

To configure HTTP RSS settings:

1. Click **HTTP** → **RSS** from the navigation menu. The HTTP RSS window opens and displays the current RSS configuration.

Figure 4-35. HTTP RSS



HTTP RSS

RSS Feed: ○ On ○ Off
Persistent: ○ On ○ Off
Max Entries:

Current Configuration

RSS Feed:	On
Persistent:	On
Max Entries:	100
Data:	72 entries (3679 bytes) [View] [Clear]

An RDF Site Summary (RSS) syndication feed is served by the HTTP Server. This feed contains up-to-date information regarding the configuration changes that occur on the device.

Specifying the RSS Feed to be **Persistent** results in the data being stored on the filesystem. The file used is "/cfg_log.txt". This allows feed data to be available across reboots (or until the factory defaults are set).

Each RSS Feed entry is prefixed with a timestamp as follows: "[BC:HH:MM:SS]". "BC" is the Boot Cycle value. This value is the number of times the device has been rebooted since the factory defaults were last loaded. The resulting "HH:MM:SS" is the time since the device booted up. This somewhat cryptic scheme is used because no Real Time Clock is available.

The RSS Feed is a scrolling feed in that only the last **Max Entries** entries are cached and viewable.

Simply register the RSS Feed within your favorite RSS aggregator and you will automatically be notified of any configuration changes that occur.

Copyright © Lantronix, Inc. 2005. All rights reserved.

2. Enter or modify the following fields:

RSS Feed	Select **On** to enable RSS feeds to an RSS publisher.
Persistent	Select **On** to enable the RSS feed to be written to a file (cfg_log.txt) and available across reboots.
Max Entries	Sets the maximum number of log entries. Only the last **Max Entries** are cached and viewable.

3. In the **Current Configuration** table, view and clear currently stored fields as necessary.

4. Click **Submit**. Changes are applied immediately to the XPort AR.

XML Configuration

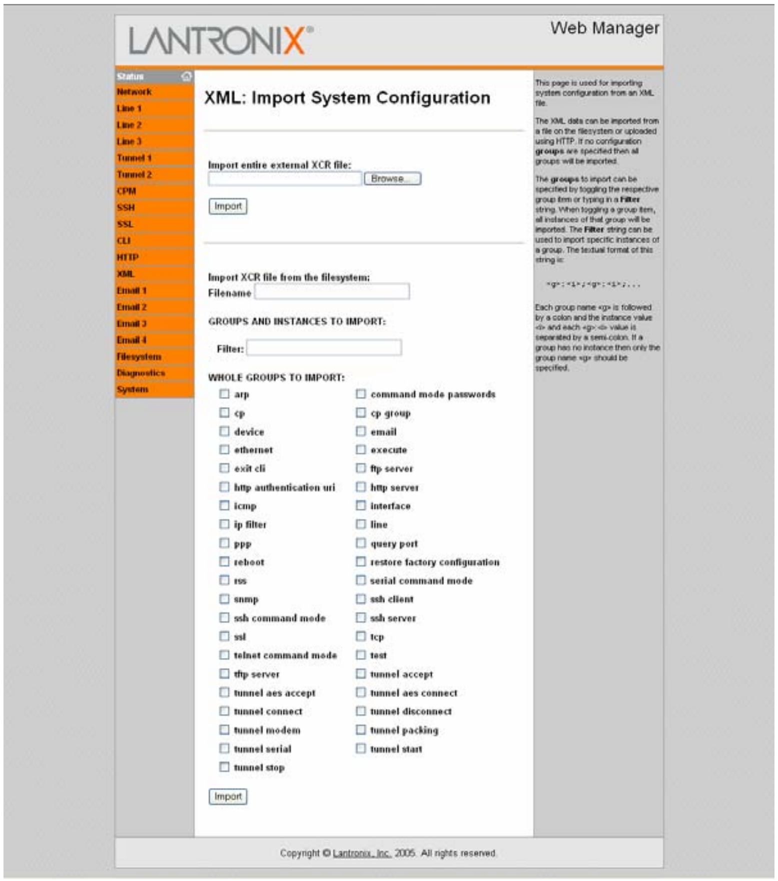
The XPort AR allows for the configuration of units using an XML configuration file. Export a current configuration for use on other XPort ARs or import a saved configuration file. For more information on using XML, see *XML* on page 134.

Import System Configuration

To import and apply an XML configuration:

1. Click **XML** → **Import** from the navigation menu. The XML: Import System Configuration window opens.

Figure 4-36. Import System Configuration



XML: Import System Configuration

Import entire external XCR file:

Import XCR file from the filesystem:
Filename

GROUPS AND INSTANCES TO IMPORT:

Filter:

WHOLE GROUPS TO IMPORT:

□ arp	□ command mode passwords
□ cp	□ cp group
□ device	□ email
□ ethernet	□ execute
□ exit cli	□ ftp server
□ http authentication uri	□ http server
□ icmp	□ interface
□ ip filter	□ line
□ ppp	□ query port
□ reboot	□ restore factory configuration
□ rss	□ serial command mode
□ snmp	□ ssh client
□ ssh command mode	□ ssh server
□ ssl	□ tcp
□ telnet command mode	□ test
□ tftp server	□ tunnel accept
□ tunnel aes accept	□ tunnel aes connect
□ tunnel connect	□ tunnel disconnect
□ tunnel modem	□ tunnel packing
□ tunnel serial	□ tunnel start
□ tunnel stop	

This page is used for importing system configuration from an XML file.

The XML data can be imported from a file on the filesystem or uploaded using HTTP. If no configuration **groups** are specified then all groups will be imported.

The **groups** to import can be specified by toggling the respective group item or typing in a **Filter** string. When toggling a group item, all instances of that group will be imported. The **Filter** string can be used to import specific instances of a group. The textual format of this string is:

```
<g>:<i>;<g>:<i>;...
```

Each group name <g> is followed by a colon and the instance value <i> and each <g>:<i> value is separated by a semi-colon. If a group has no instance then only the group name <g> should be specified.

Copyright © Lantronix, Inc. 2005. All rights reserved.

2. Use one of the following methods to import the XCR file:

   a) To import an XCR file from the filesystem, select **Import XCR file from the filesystem** and enter the filename on the XPort AR containing the file to import.

   b) To import an external file, select **Import external XCR file** and click **Browse**. Locate the file in the Choose File window.

3. (Optional) Enter the filter to apply in the **Filter** field. This selects the groups to import. The format of the input is:

   ```
   <g>:<i>;<g>:<i>; …
   ```

   Each group name (<g>) is followed by a colon (:) and the instance value (<i>). Each set of these ends with a semi-colon (;). If a group has no instance, specify only the group name (<g>).

4. Select from the list of checkboxes the groups to import. If no groups are selected, all the groups will be imported.

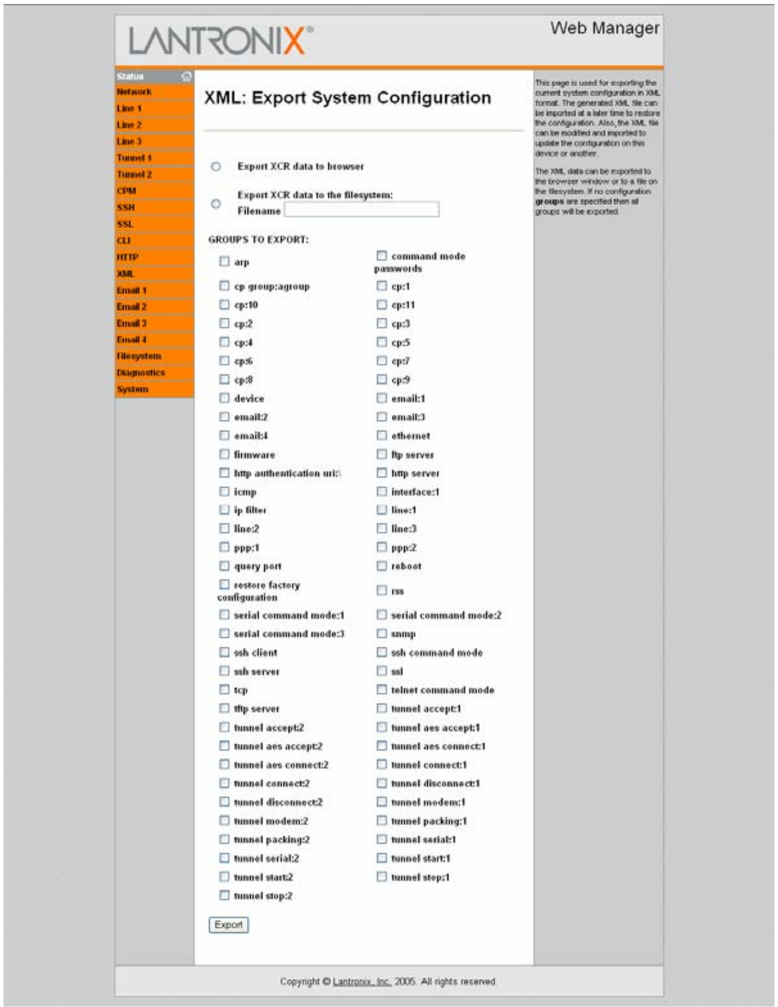
5. Click **Import**. The settings for the groups selected are applied to the XPort AR.

Export System Configuration

To export and store an XPort AR's configuration:

1. Click **XML → Export** from the navigation menu. The XML: Export System Configuration window opens.

Figure 4-37. Export System Configuration



XML: Export System Configuration

○ Export XCR data to browser

○ Export XCR data to the filesystem:
Filename

GROUPS TO EXPORT:

□ arp	□ command mode passwords
□ cp group:agroup	□ cp:1
□ cp:10	□ cp:11
□ cp:2	□ cp:3
□ cp:4	□ cp:5
□ cp:6	□ cp:7
□ cp:8	□ cp:9
□ device	□ email:1
□ email:2	□ email:3
□ email:4	□ ethernet
□ firmware	□ ftp server
□ http authentication uri:\	□ http server
□ icmp	□ interface:1
□ ip filter	□ line:1
□ line:2	□ line:3
□ ppp:1	□ ppp:2
□ query port	□ reboot
□ restore factory configuration	□ rss
□ serial command mode:1	□ serial command mode:2
□ serial command mode:3	□ snmp
□ ssh client	□ ssh command mode
□ ssh server	□ ssl
□ tcp	□ telnet command mode
□ tftp server	□ tunnel accept:1
□ tunnel accept:2	□ tunnel aes accept:1
□ tunnel aes accept:2	□ tunnel aes connect:1
□ tunnel aes connect:2	□ tunnel connect:1
□ tunnel connect:2	□ tunnel disconnect:1
□ tunnel disconnect:2	□ tunnel modem:1
□ tunnel modem:2	□ tunnel packing:1
□ tunnel packing:2	□ tunnel serial:1
□ tunnel serial:2	□ tunnel start:1
□ tunnel start:2	□ tunnel stop:1
□ tunnel stop:2	

This page is used for exporting the current system configuration in XML format. The generated XML file can be imported at a later time to restore the configuration. Also, the XML file can be modified and imported to update the configuration on this device or another.

The XML data can be exported to the browser window or to a file on the filesystem. If no configuration **groups** are specified then all groups will be exported.

Copyright © Lantronix, Inc. 2005. All rights reserved.

2. Use one of the following methods to export the XCR file:

   a) To view the XCR data (without storing it), select **Export ECR data to browser**.

   b) To export to a file on the XPort AR filesystem, select **Export XCR data to the filesystem**. In the text box, enter the name for the file. The system will create the file and store it in the root directory of the XPort AR.

3. Select from the list of checkboxes the groups to export. If no groups are selected, all the groups will be exported.

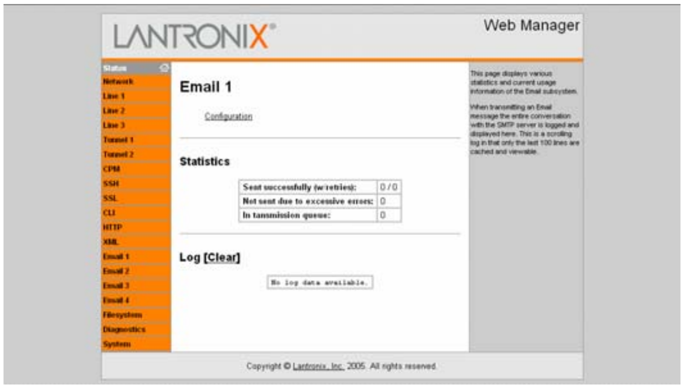
4. Click Export. The groups display if exporting the data to the browser. If exporting to the filesystem, the files are stored on the filesystem. (To view these files or store them elsewhere, see *Filesystem Configuration* on page 56.)

Email Configuration

The XPort AR allows for the configuration of four email alerts relating to the Configuration Pins (CPs). Select the **Email** link on the left menu bar to display the **Email** menu and statistics.

*Note: The following section describes the steps to configure **Email 1**; these steps also apply to **Email 2**, **Email 3**, and **Email 4** menu options.*

Figure 4-38. Email Statistics



Email 1

Statistics

Sent successfully (w/retries):	0 / 0
Not sent due to excessive errors:	0
In tansmission queue:	0

Log [Clear]

```
No log data available.
```

This page displays various statistics and current usage information of the Email subsystem.

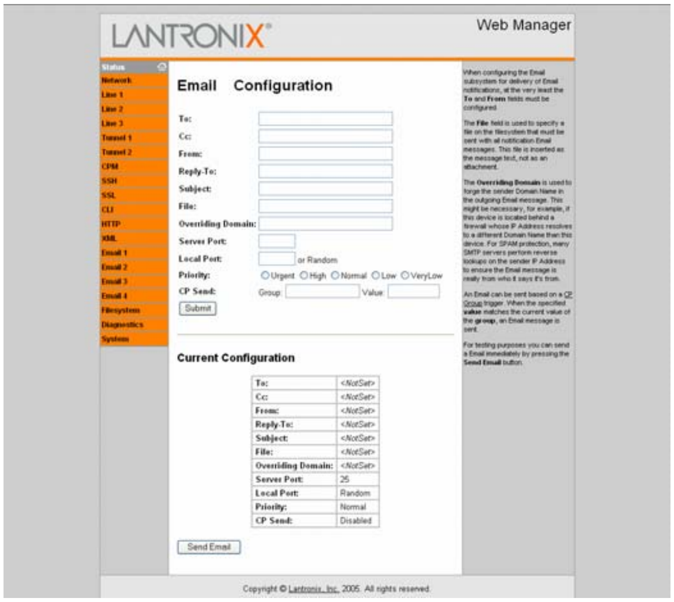
When transmitting an Email message the entire conversation with the SMTP server is logged and displayed here. This is a scrolling log in that only the last 100 lines are cached and viewable.

Copyright © Lantronix, Inc. 2005. All rights reserved.

To configure XPort AR's email settings:

1. Click **Email → Configuration** from the navigation menu. The Email Configuration window opens and displays the current Email configuration.

Figure 4-39. Email Configuration



Email Configuration

To:
Cc:
From:
Reply-To:
Subject:
File:
Overriding Domain:
Server Port:
Local Port: or Random
Priority: ○ Urgent ○ High ○ Normal ○ Low ○ VeryLow
CP Send: Group: Value:

Current Configuration

To:	<NotSet>
Cc:	<NotSet>
From:	<NotSet>
Reply-To:	<NotSet>
Subject:	<NotSet>
File:	<NotSet>
Overriding Domain:	<NotSet>
Server Port:	25
Local Port:	Random
Priority:	Normal
CP Send:	Disabled

When configuring the Email subsystem for delivery of Email notifications, at the very least the **To** and **From** fields must be configured.

The **File** field is used to specify a file on the filesystem that must be sent with all notification Email messages. This file is inserted as the message text, not as an attachment.

The **Overriding Domain** is used to forge the sender Domain Name in the outgoing Email message. This might be necessary, for example, if this device is located behind a firewall whose IP Address resolves to a different Domain Name than this device. For SPAM protection, many SMTP servers perform reverse lookups on the sender IP Address to ensure the Email message is really from who it says it's from.

An Email can be sent based on a CP Group trigger. When the specified **value** matches the current value of the **group**, an Email message is sent.

For testing purposes you can send a Email immediately by pressing the **Send Email** button.

Copyright © Lantronix, Inc. 2005. All rights reserved.

2. Enter or modify the following fields:

To	Enter the email address to which the email alerts will be sent.
CC	Enter the email address to which the email alerts will be CC'ed.
From	Enter the email address to list in the From field of the email alert.
Reply-To	Enter the email address to list in the Reply-To field of the email alert.
Subject	Enter the subject for the email alert.
File	Enter the path of the file to send with the email alert. This file displays within the message body of the email.
Overriding Domain	Enter the domain name to override the current domain name in EHLO (Extended Hello).
Server Port	Enter the SMTP server port number. The default is a random port number.
Local Port	Enter the local port to use for email alerts.
Priority	Select the priority level for the email alert.
CP Send	Configure this field to send an email based on a CP Group trigger. An email is sent when the specified **Value** matches the current **Group**'s value.

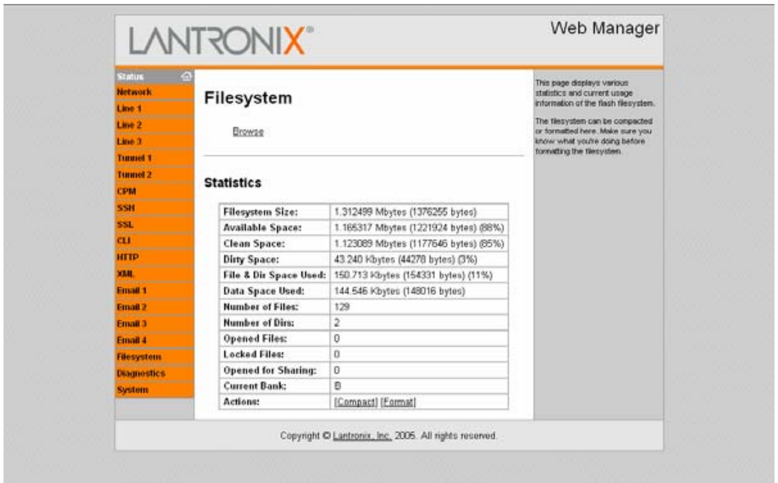
3. In the **Current Configuration** table, delete currently stored fields as necessary.

4. Click **Submit**. Changes are applied immediately to the XPort AR.

Filesystem Configuration

The XPort AR uses a flash filesystem to store files. Use the Filesystem option to view current file diagnostics or modify files.

Figure 4-40. Filesystem



Filesystem

Statistics

Filesystem Size:	1.312499 Mbytes (1376255 bytes)
Available Space:	1.166317 Mbytes (1221924 bytes) (88%)
Clean Space:	1.123089 Mbytes (1177646 bytes) (85%)
Dirty Space:	43.240 Kbytes (44278 bytes) (3%)
File & Dir Space Used:	150.713 Kbytes (154331 bytes) (11%)
Data Space Used:	144.546 Kbytes (148016 bytes)
Number of Files:	129
Number of Dirs:	2
Opened Files:	0
Locked Files:	0
Opened for Sharing:	0
Current Bank:	B
Actions:	[Compact] [Format]

This page displays various statistics and current usage information of the flash filesystem.

The filesystem can be compacted or formatted here. Make sure you know what you're doing before formatting the filesystem.

Copyright © Lantronix, Inc. 2005. All rights reserved.

To compact or format the XPort AR's filesystem:

1. Click **Filesystem** from the navigation menu. The Filesystem window opens and displays the current filesystem statistics and usage.

2. To compact the files, click **Compact.**

   Note: *Data can be lost if power is cycled when compacting the filesystem.*

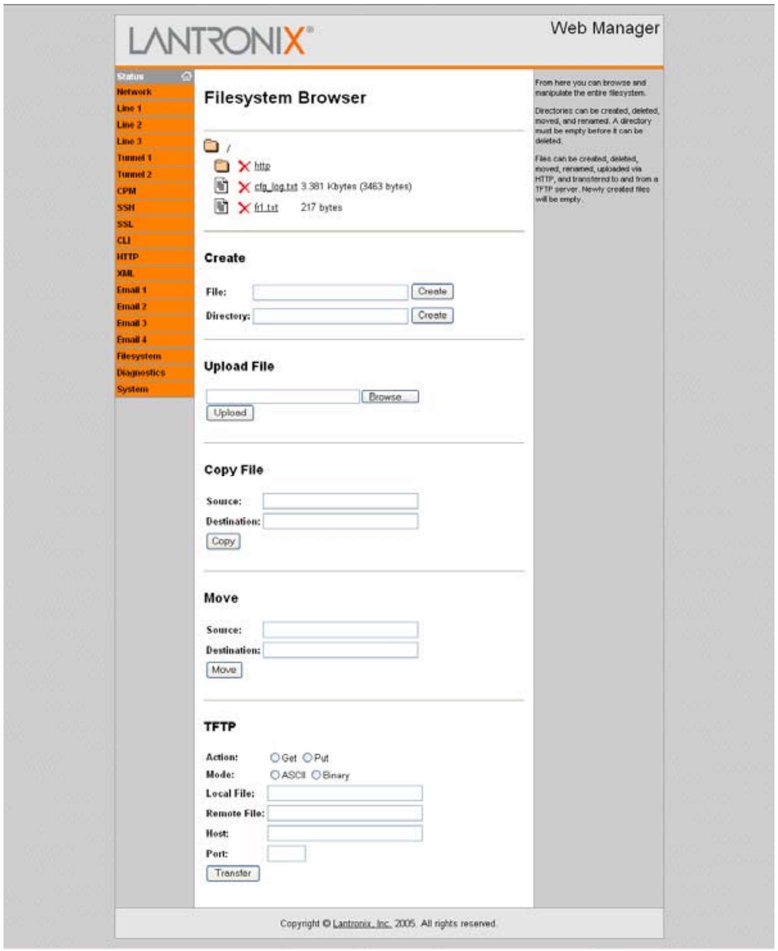
3. To reformat the filesystem, click **Format**.

   Note: *All files and configuration settings on the filesystem are destroyed upon formatting, including Web Manager files. Back up all files as necessary. Upon formatting, the current configuration is lost.*

To browse the XPort AR's filesystem:

1. Click **Filesystem → Browse** from the navigation menu. The Filesystem Browser window opens and displays the current filesystem configuration.

Figure 4-41. Filesystem Browser



Filesystem Browser

/
- http
- cfg_log.txt 3.381 Kbytes (3463 bytes)
- fr1.txt 217 bytes

Create

File: Create

Directory: Create

Upload File

Browse...

Upload

Copy File

Source:

Destination:

Copy

Move

Source:

Destination:

Move

TFTP

Action: ○ Get ○ Put

Mode: ○ ASCII ○ Binary

Local File:

Remote File:

Host:

Port:

Transfer

From here you can browse and manipulate the entire filesystem.

Directories can be created, deleted, moved, and renamed. A directory must be empty before it can be deleted.

Files can be created, deleted, moved, renamed, uploaded via HTTP, and transferred to and from a TFTP server. Newly created files will be empty.

Copyright © Lantronix, Inc. 2005. All rights reserved.

2. Click on a filename to view the contents.

3. Click the **X** next to a filename to delete the file or directory. A directory can only be deleted if it is empty.

4. Enter or modify the following fields:

Note: *Changes apply to the current directory view. To make changes within other folders, click on the folder or directory and then enter the parameters in the fields listed below.*

Create

File	Enter a filename and click **Create**. The XPort AR creates the empty file (0 bytes) and stores it in the current directory.
Directory	Enter a folder name and click **Create**. The XPort AR creates the folder and stores it in the current directory.

Upload File

Browse	Click **Browse** and locate the file to upload to the current filesystem directory. Click **Upload** to complete the process.

Copy File

Source	Enter the filename to copy.
Destination	Enter the folder where the **Source** file will be copied. Click **Copy** to complete the process. ***Note:*** *The **Source** and **Destination** filenames can be different.*

Move

Source	Enter the filename to move.
Destination	Enter the folder into which the **Source** file will be moved. Click **Move** to complete the process. ***Note:*** *When the **Source** and **Destination** filenames are different, the file and folder are renamed.*

TFTP

Action	Select **Get** or **Put**. Choose **Get** to receive a file. Choose **Put** to send a file.
Mode	Select **ASCII** or **Binary**.
Local File	Enter the name of the file to send to the remote location (**Put**) or to store locally (**Get**).
Remote File	Enter the name of the file on the remote location to store externally (**Put**) or to store locally (**Get**).
Host	Enter the IP address or hostname of the remote location.
Port	Enter the port number for TFTP communication. Click **Transfer** to complete the file transfer. The default is port 69.

Diagnostics Configuration

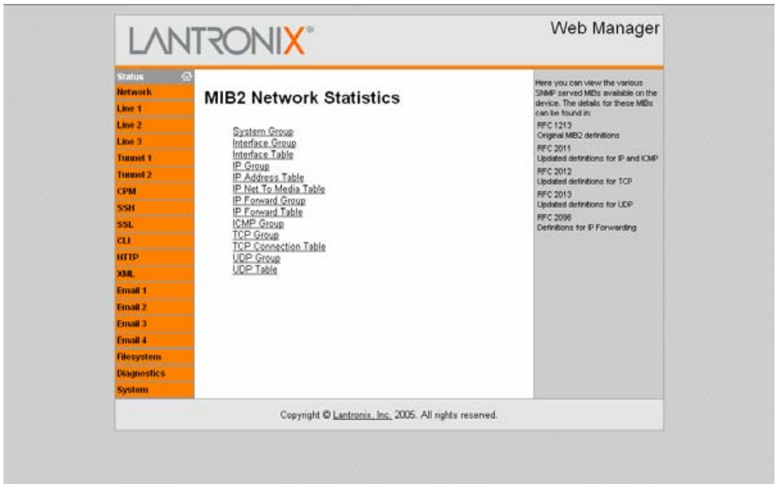
The XPort AR has several tools for diagnostics and statistics. Select the **Diagnostics** link on the left menu bar to display the **Diagnostics** menu. The sub-menus allow for the configuration or viewing of MIB2 statistics, IP socket information, ping, traceroute, DNS lookup, memory, buffer pools, processes, and hardware.

MIB2 Statistics

To view XPort AR's MIB2 statistics:

1. Click **Diagnostics → MIB2 Statistics** from the navigation menu. The MIB2 Network Statistics window opens.

Figure 4-42. MIB2 Network Statistics



MIB2 Network Statistics

System Group
Interface Group
Interface Table
IP Group
IP Address Table
IP Net To Media Table
IP Forward Group
IP Forward Table
ICMP Group
TCP Group
TCP Connection Table
UDP Group
UDP Table

Here you can view the various SNMP served MIBs available on the device. The details for these MIBs can be found in:

RFC 1213
Original MIB2 definitions
RFC 2011
Updated definitions for IP and ICMP
RFC 2012
Updated definitions for TCP
RFC 2013
Updated definitions for UDP
RFC 2096
Definitions for IP Forwarding

Copyright © Lantronix, Inc. 2005. All rights reserved.

2. Click on any of the available links to open the corresponding table and statistics. For more information, refer to the following Requests for Comments (RFCs):

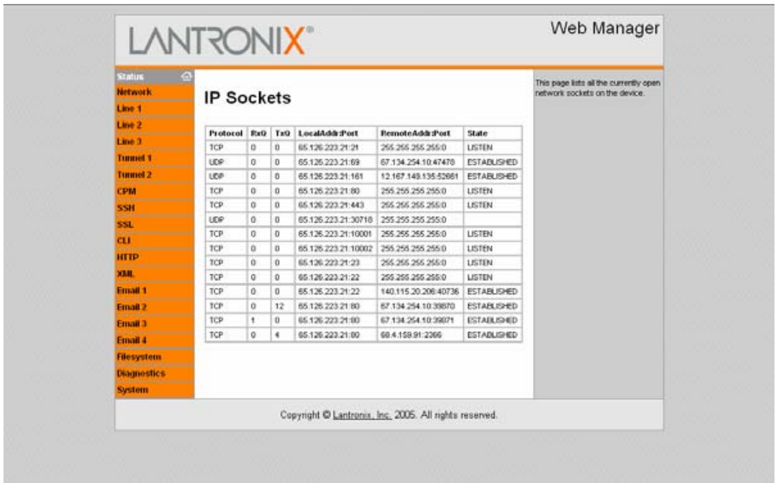
RFC 1213	Original MIB2 definitions.
RFC 2011	Updated definitions for IP and ICMP.
RFC 2012	Updated definitions for TCP.
RFC 2013	Updated definitions for UDP.
RFC 2096	Definitions for IP forwarding.

IP Sockets

To display open network sockets on the XPort AR:

1. Click **Diagnostics → IP Sockets** from the navigation menu. The IP Sockets window opens and displays all of the open network sockets on the XPort AR.

Figure 4-43. IP Sockets



IP Sockets

Protocol	RxQ	TxQ	LocalAddr:Port	RemoteAddr:Port	State
TCP	0	0	65.126.223.21:21	255.255.255.255:0	LISTEN
UDP	0	0	65.126.223.21:69	67.134.254.10:47478	ESTABLISHED
UDP	0	0	65.126.223.21:161	12.167.149.135:52661	ESTABLISHED
TCP	0	0	65.126.223.21:80	255.255.255.255:0	LISTEN
TCP	0	0	65.126.223.21:443	255.255.255.255:0	LISTEN
UDP	0	0	65.126.223.21:30718	255.255.255.255:0	
TCP	0	0	65.126.223.21:10001	255.255.255.255:0	LISTEN
TCP	0	0	65.126.223.21:10002	255.255.255.255:0	LISTEN
TCP	0	0	65.126.223.21:23	255.255.255.255:0	LISTEN
TCP	0	0	65.126.223.21:22	255.255.255.255:0	LISTEN
TCP	0	0	65.126.223.21:22	140.115.20.206:40736	ESTABLISHED
TCP	0	12	65.126.223.21:80	67.134.254.10:39870	ESTABLISHED
TCP	1	0	65.126.223.21:80	67.134.254.10:39871	ESTABLISHED
TCP	0	4	65.126.223.21:80	69.4.159.91:2366	ESTABLISHED

This page lists all the currently open network sockets on the device.

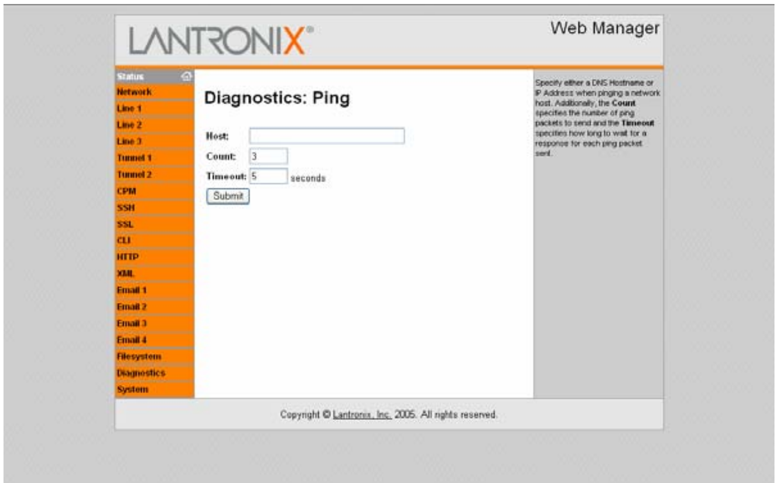
Copyright © Lantronix, Inc. 2005. All rights reserved.

Ping

To ping a remote device or computer:

2. Click **Diagnostics → Ping** from the navigation menu. The Diagnostics: Ping window opens.

Figure 4-44. Diagnostics: Ping



Diagnostics: Ping

Host:

Count: 3

Timeout: 5 seconds

Specify either a DNS Hostname or IP Address when pinging a network host. Additionally, the **Count** specifies the number of ping packets to send and the **Timeout** specifies how long to wait for a response for each ping packet sent.

Copyright © Lantronix, Inc. 2005. All rights reserved.

3. Enter or modify the following fields:

Host	Enter the IP address for the XPort AR to ping.
Count	Enter the number of ping packets XPort AR should attempt to send to the **Host**. The default is 3.
Timeout	Enter the time, in seconds, for the XPort AR to wait for a response from the host before timing out. The default is 5 seconds.

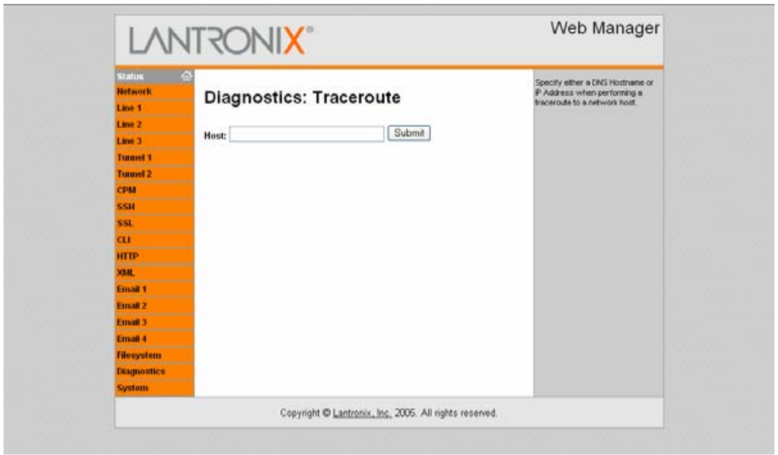
4. Click **Submit**. The results of the ping display in the window.

Traceroute

To use traceroute from the XPort AR:

1. Click **Diagnostics → Traceroute** from the navigation menu. The Diagnostics: Traceroute window opens.

Figure 4-45. Diagnostics: Traceroute



Diagnostics: Traceroute

Specify either a DNS Hostname or IP Address when performing a traceroute to a network host.

2. Enter or modify the following fields:

Traceroute	Enter the IP address or DNS hostname. This address is used to show the path between it and the XPort AR when issuing the traceroute command.

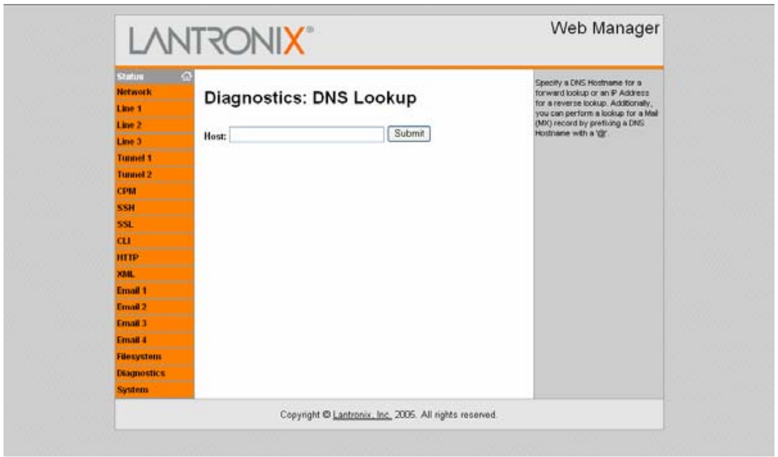
3. Click **Submit**. The results of the traceroute display in the window.

DNS Lookup

To use forward or reverse DNS lookup:

1. Click **Diagnostics → DNS Lookup** from the navigation menu. The Diagnostics: DNS Lookup window opens.

Figure 4-46. Diagnostics: DNS Lookup



Diagnostics: DNS Lookup

Specify a DNS Hostname for a forward lookup or an IP Address for a reverse lookup. Additionally, you can perform a lookup for a Mail (MX) record by prefixing a DNS Hostname with a '@'.

2. Enter or modify the following field:

Lookup	Enter an IP address for reverse lookup to locate the hostname for that IP address. Enter a hostname for forward lookup to locate the corresponding IP address. Enter a domain name (prefixed with "@") to look up the Mail Exchange (MX) record IP address.

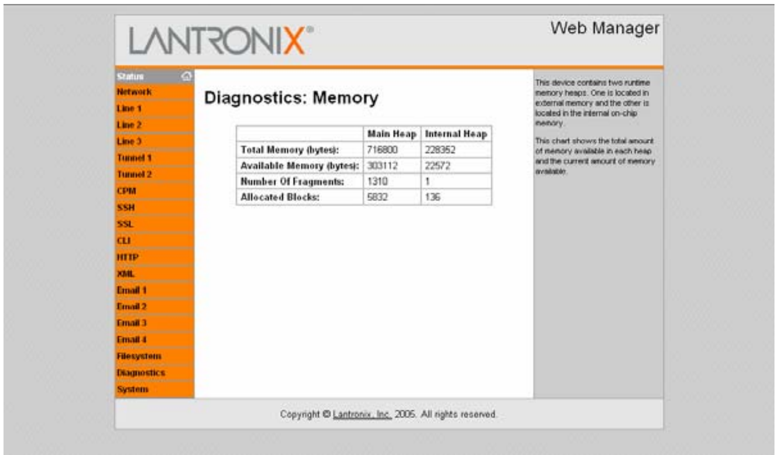
3. Click **Submit**. The results of the lookup display in the window.

Memory

To display memory statistics for the XPort AR:

1. Click **Diagnostics → Memory** from the navigation menu. The Diagnostics: Memory window displays.

Figure 4-47. Diagnostics: Memory



Diagnostics: Memory

	Main Heap	Internal Heap
Total Memory (bytes):	716800	228352
Available Memory (bytes):	303112	22572
Number Of Fragments:	1310	1
Allocated Blocks:	5832	136

This device contains two runtime memory heaps. One is located in external memory and the other is located in the internal on-chip memory.

This chart shows the total amount of memory available in each heap and the current amount of memory available.

Copyright © Lantronix, Inc. 2005. All rights reserved.

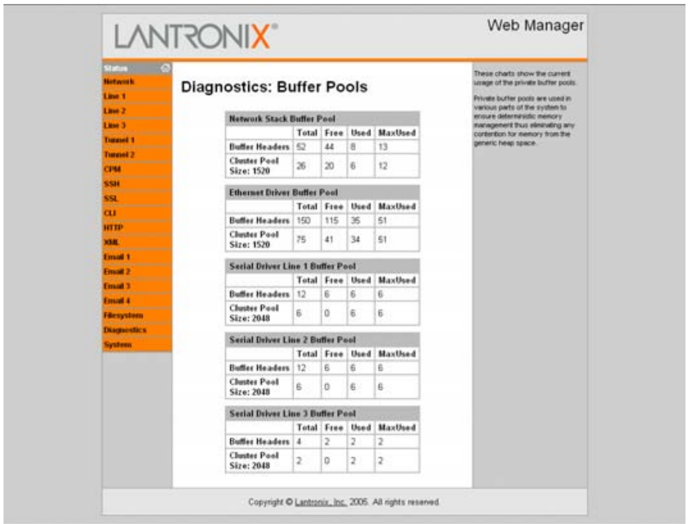
Buffer Pools

Several parts of the XPort AR system use private buffer pools to ensure deterministic memory management.

To display the XPort AR's buffer pools:

1. Click **Diagnostics → Processes** from the navigation menu. The Diagnostics: Buffer Pools window opens.

Figure 4-48. Diagnostics: Buffer Pools



Diagnostics: Buffer Pools

Network Stack Buffer Pool				
	Total	Free	Used	MaxUsed
Buffer Headers	52	44	8	13
Cluster Pool Size: 1520	26	20	6	12

Ethernet Driver Buffer Pool				
	Total	Free	Used	MaxUsed
Buffer Headers	150	115	35	51
Cluster Pool Size: 1520	75	41	34	51

Serial Driver Line 1 Buffer Pool				
	Total	Free	Used	MaxUsed
Buffer Headers	12	6	6	6
Cluster Pool Size: 2048	6	0	6	6

Serial Driver Line 2 Buffer Pool				
	Total	Free	Used	MaxUsed
Buffer Headers	12	6	6	6
Cluster Pool Size: 2048	6	0	6	6

Serial Driver Line 3 Buffer Pool				
	Total	Free	Used	MaxUsed
Buffer Headers	4	2	2	2
Cluster Pool Size: 2048	2	0	2	2

These charts show the current usage of the private buffer pools.

Private buffer pools are used in various parts of the system to ensure deterministic memory management thus eliminating any contention for memory from the generic heap space.

Copyright © Lantronix, Inc. 2005. All rights reserved.

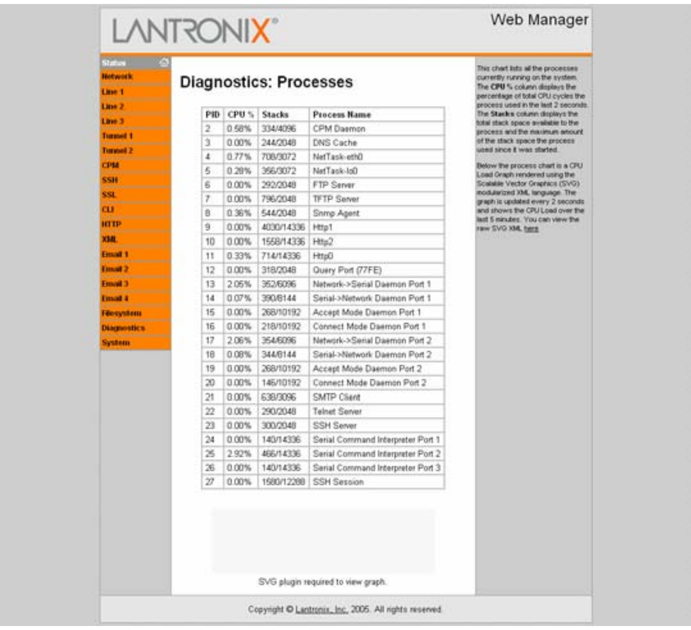
Processes

The XPort AR Processes window displays all the processes currently running on the system. It displays the Process ID (PID), the percentage of total CPU cycles a process used within the last 2 seconds, the total stack space available, the maximum amount of stack space used by the process since it started, and the process name.

To display the processes running on the XPort AR and their associated statistics:

1. Click **Diagnostics → Processes** from the navigation menu. The Diagnostics: Processes window opens.

Figure 4-49. Diagnostics: Processes



Diagnostics: Processes

PID	CPU %	Stacks	Process Name
2	0.58%	334/4096	CPM Daemon
3	0.00%	244/2048	DNS Cache
4	0.77%	708/3072	NetTask-eth0
5	0.28%	356/3072	NetTask-lo0
6	0.00%	292/2048	FTP Server
7	0.00%	796/2048	TFTP Server
8	0.36%	544/2048	Snmp Agent
9	0.00%	4030/14336	Http1
10	0.00%	1558/14336	Http2
11	0.33%	714/14336	Http0
12	0.00%	318/2048	Query Port (77FE)
13	2.05%	352/6096	Network->Serial Daemon Port 1
14	0.07%	390/8144	Serial->Network Daemon Port 1
15	0.00%	268/10192	Accept Mode Daemon Port 1
16	0.00%	218/10192	Connect Mode Daemon Port 1
17	2.06%	354/6096	Network->Serial Daemon Port 2
18	0.08%	344/8144	Serial->Network Daemon Port 2
19	0.00%	268/10192	Accept Mode Daemon Port 2
20	0.00%	146/10192	Connect Mode Daemon Port 2
21	0.00%	638/3096	SMTP Client
22	0.00%	290/2048	Telnet Server
23	0.00%	300/2048	SSH Server
24	0.00%	140/14336	Serial Command Interpreter Port 1
25	2.92%	466/14336	Serial Command Interpreter Port 2
26	0.00%	140/14336	Serial Command Interpreter Port 3
27	0.00%	1580/12288	SSH Session

SVG plugin required to view graph.

This chart lists all the processes currently running on the system. The **CPU %** column displays the percentage of total CPU cycles the process used in the last 2 seconds. The **Stacks** column displays the total stack space available to the process and the maximum amount of the stack space the process used since it was started.

Below the process chart is a CPU Load Graph rendered using the Scalable Vector Graphics (SVG) modularized XML language. The graph is updated every 2 seconds and shows the CPU Load over the last 5 minutes. You can view the raw SVG XML here.

Copyright © Lantronix, Inc. 2005. All rights reserved.

Note: *The Adobe SVG plug-in is required to view the CPU Load Graph.*

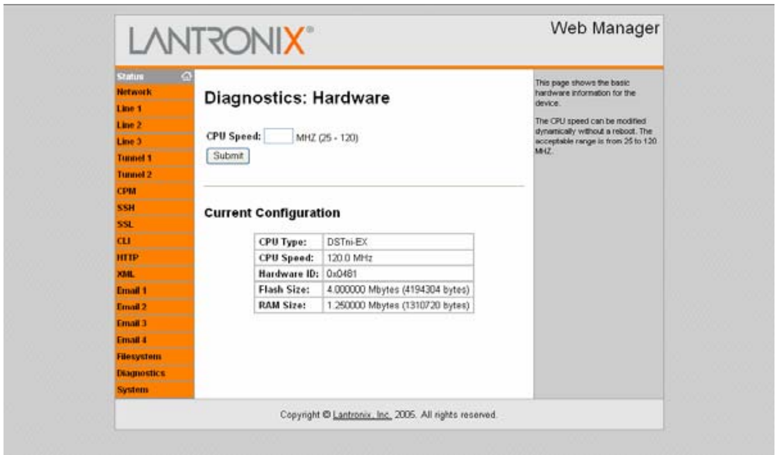
Hardware

The Hardware window displays basic hardware information and allows for the modification of the CPU speed.

To display the XPort AR's hardware diagnostics:

1. Click **Diagnostics → Hardware** from the navigation menu. The Diagnostics: Hardware window opens and displays current the current hardware configuration.

Figure 4-50. Diagnostics: Hardware



Diagnostics: Hardware

CPU Speed: MHZ (25 - 120)

Current Configuration

CPU Type:	DSTni-EX
CPU Speed:	120.0 MHz
Hardware ID:	0x0481
Flash Size:	4.000000 Mbytes (4194304 bytes)
RAM Size:	1.250000 Mbytes (1310720 bytes)

This page shows the basic hardware information for the device.

The CPU speed can be modified dynamically without a reboot. The acceptable range is from 25 to 120 MHZ.

Copyright © Lantronix, Inc. 2005. All rights reserved.

2. Enter or modify the following field:

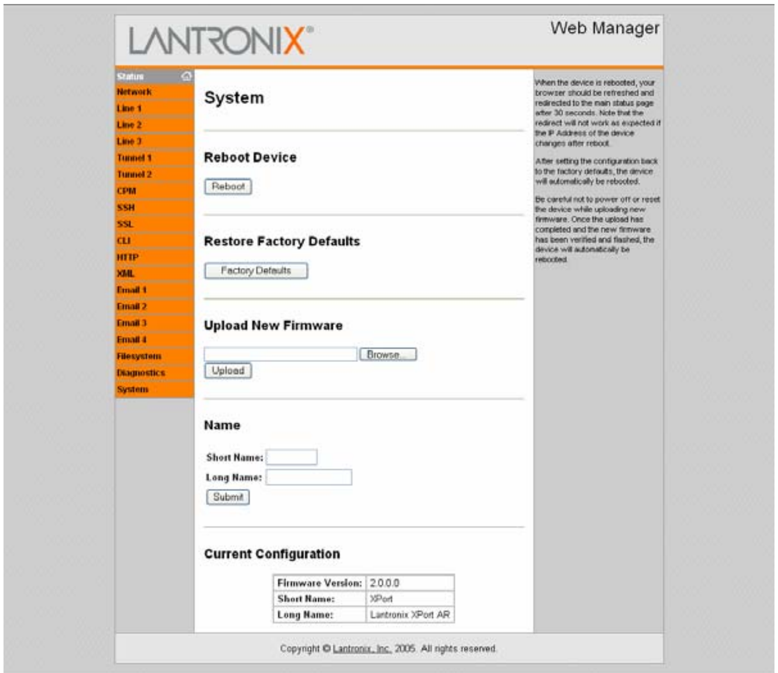
CPU Speed	Enter the XPort AR's CPU speed. Accepted values are between 25 and 120 MHz.

4. Click **Submit**. The CPU speed is updated immediately (no reboot required).

System Configuration

The XPort AR System window allows for rebooting the device, restoring factory defaults, uploading new firmware, configuring the short and long name, and viewing the current system configuration.

Figure 4-51. System



System

Reboot Device

Restore Factory Defaults

Upload New Firmware

Name

Short Name:

Long Name:

Current Configuration

Firmware Version:	2.0.0.0
Short Name:	XPort
Long Name:	Lantronix XPort AR

When the device is rebooted, your browser should be refreshed and redirected to the main status page after 30 seconds. Note that the redirect will not work as expected if the IP Address of the device changes after reboot.

After setting the configuration back to the factory defaults, the device will automatically be rebooted.

Be careful not to power off or reset the device while uploading new firmware. Once the upload has completed and the new firmware has been verified and flashed, the device will automatically be rebooted.

Copyright © Lantronix, Inc. 2005. All rights reserved.

To configure the XPort AR's system settings:

1. Click **System** from the navigation menu. The System window opens.
2. Configure the XPort AR's system using the following fields:

Reboot Device	Click **Reboot** to reboot the XPort AR. The system refreshes and redirects the browser to the XPort AR's home page.
Restore Factory Defaults	Click **Factory Defaults** to restore the XPort AR to the original factory settings. All configurations will be lost. The XPort AR automatically reboots upon setting back to the defaults.
Upload New Firmware	Click **Browse** to locate the firmware file location. Click **Upload** to install the firmware on the XPort AR. The device automatically reboots upon the installation of new firmware.
Name	Enter a new **Short Name** and a **Long Name** (if necessary). The **Short Name** is a maximum of 8 characters. Changes take place upon the next reboot.

5: Configuration Using Telnet or Serial Port

Configure the XPort AR so that it can communicate on a network with your serial device. For example, set the way the unit responds to serial and network traffic, how it handles serial packets, and when to start or close a connection.

As an alternative to using Web Manager, configure the XPort AR using a series of prompts referred to as Command Mode, accessed through a Telnet or a serial port connection.

The configuration may be changed at any time. Changes are applied immediately to the XPort AR (except for network configurations, which require a reboot).

This chapter provides instructions on using Command Mode and detailed explanations of the available commands.

Accessing Command Mode

Using Telnet

To configure the unit over the network, establish a Telnet connection.

Note: As an alternative, establish a Telnet connection by clicking the ***Telnet*** *tab in the DeviceInstaller. See Using DeviceInstaller on page 15.*

1. From the Windows Start menu, click **Run** and type the following command, where x.x.x.x is the IP address:

```
telnet x.x.x.x
```

2. Click **OK**. Upon connection, enter “!” multiple times until one character appears on screen.
3. Enter “xyz” to enter Command Mode.

Using the Serial Port

For local configuration, connect a terminal or a PC running a terminal emulation program to the unit’s serial port. Configure the terminal (or emulation) for 9600 baud, 8-bit, no parity, 1 stop bit, and no flow control.

1. Cycle the unit’s power (power off and back on). After power-up, the self-test begins and the diagnostic and status LEDs start blinking.
2. Click **OK**. Upon connection, enter “!” multiple times until one character appears on screen.
3. Enter “xyz” to enter Command Mode.

Navigating the Command Line Interface

Commands at the root level (top level) of the CLI do not affect current configuration settings. Commands within the Enable menu (and its sub-menus) modify the XPort AR's configuration.

Items within < > (e.g. <string>) are required parameters.

To view acceptable commands enter "**?**".

To move to a sub-level and traverse the tree of commands, enter each sub-command only in its parent command prompt. For example, to access the Tunnel1 level within the Enable level (which is below the root level), enter:

```
root>enable
root(enable)#tunnel1
```

To exit and return to the menu one level higher, type **exit**.

The following key combinations are permitted when configuring the XPort AR from the CLI:

- **Ctrl + a:** place cursor at the beginning of line
- **Ctrl + b:** backspace one character
- **Ctrl + d:** delete one character
- **Ctrl + e:** place cursor at the end of the line
- **Ctrl + f:** move cursor forward one character
- **Ctrl + k:** delete everything to the end of the line
- **Ctrl + l:** redraw the command line
- **Ctrl + n:** display the next line in the history
- **Ctrl + p:** display the previous line in the history
- **Ctrl + u:** delete entire line and place cursor at start of prompt
- **Ctrl + w:** delete one word back in line
- **Esc + b:** move cursor back one word
- **Esc + f:** move cursor forward one word

Note: *The XPort AR CLI also supports tab completion.*

To view the current configuration at any level:

- Type `show`. The configuration for that menu level displays.

To view the list of commands available at the current menu level:

- At the command prompt, enter `?`. The list of current commands displays.

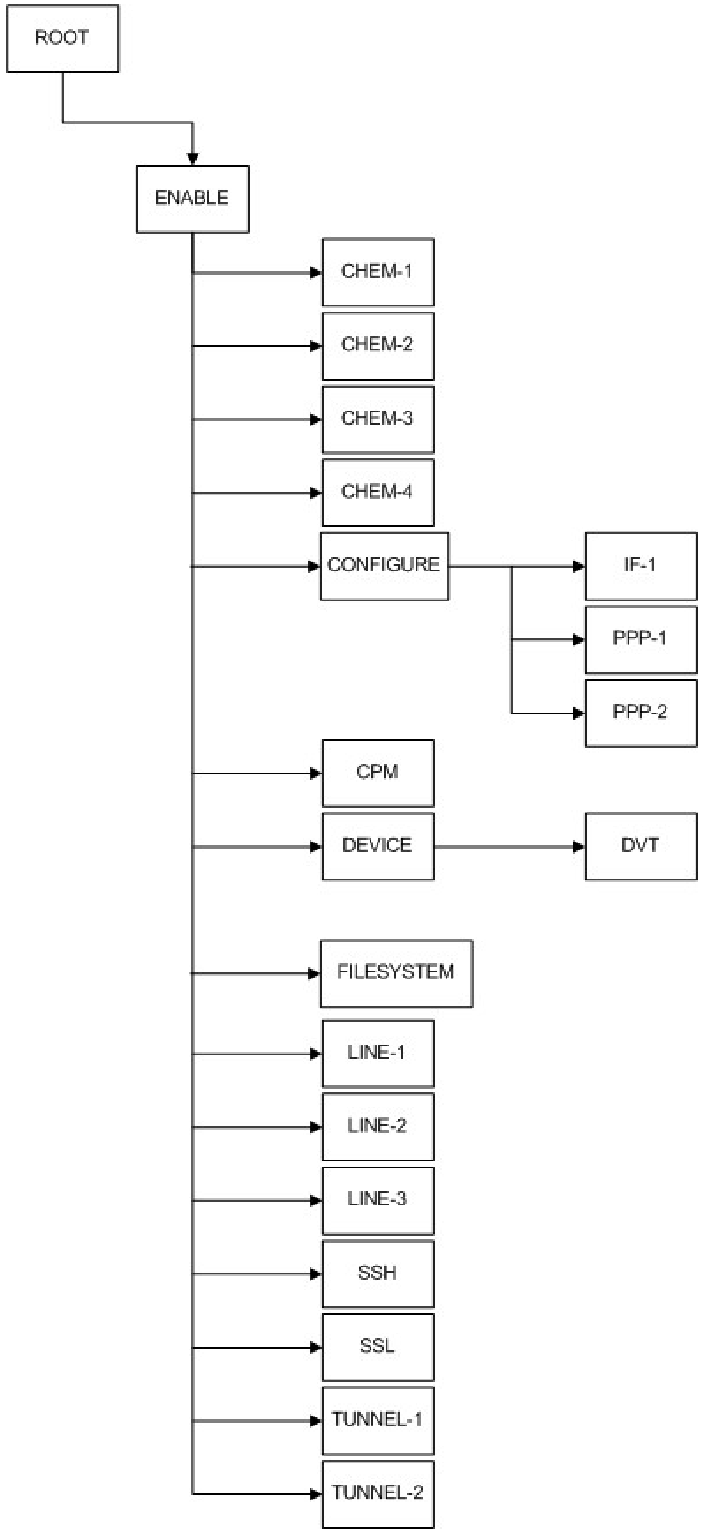
To return to the next level up in the menu hierarchy:

- At the command prompt, type **exit**. The prompt for the parent menu displays.

To view the available commands and their explanation:

- At the command prompt, type `*`. The list of commands for that menu level and their description displays.

XPort AR CLI Level Hierarchy



Root Configuration Menu

Top level root commands do not alter the configuration of the XPort AR.

`Clrscrn`

Clears the screen.

`Enable`

Displays the Enable level prompt. Within this menu, changes can be written to the XPort AR. For the list of Enable prompts, see *Enable Menu* on page 70.

`Exit`

Exit from the system.

`Ping <host>`

Pings the **host** destination 5 times with a 5 second timeout.

`Ping <host> <count>`

Pings the **host** destination the specified number of times (**count**) with a 5 second timeout.

`Ping <host> <count> <timeout>`

Pings the **string** destination the specified number of times (**count**) with a specified **timeout** (in seconds).

`Show history`

Shows the set of commands inputted from the moment user was brought back up to this menu. Entering a sub-menu, and then returning to this menu displays only the commands inputted since re-entering this command set.

`Show XPort`

Shows current XPort AR settings.

`Trace route <host>`

Determines the path taken from a computer to a specified destination. Enter the destination IP address.

Enable Menu

The following sections describe the configurable parameters within the Enable configuration menu.

`Auto show interfaces`

Displays interface statistics.

`Auto show processes`

Continuously displays thread runtime information.

`Chem`

Change from the Enable menu to the Configure Email 1 (Chem) sub-menu. For the list of Chem prompts, see *Chem Menu* on page 74.

`Chem 1`

Change from the Enable menu to the Configure Email 1 (Chem) sub-menu. For the list of Chem prompts, see *Chem Menu* on page 74.

`Chem 2`

Change from the Enable menu to the Configure Email 2 (Chem) sub-menu. For the list of Chem prompts, see *Chem Menu* on page 74.

`Chem 3`

Change from the Enable menu to the Configure Email 3 (Chem) sub-menu. For the list of Chem prompts, see *Chem Menu* on page 74.

`Chem 4`

Change from the Enable menu to the Configure Email 4 (Chem) sub-menu. For the list of Chem prompts, see *Chem Menu* on page 74.

`Clear interface counters`

Sets to zero the interface session counters.

`Clear line <number>`

Use the **`show sessions`** command to view the active command mode sessions on the XPort AR. Each session is assigned a number. Use the **`clear line`** command to end a specific command mode session.

`Clear query port counters`

Sets to zero the Query Port counters.

`Clear ssh <session>`

Ends an active SSH session on the XPort AR.

`Clear telnet <session>`

Ends an active Telnet session on the XPort AR.

`Configure`

Displays the Configuration level menu. For the list of commands within this menu, see *Configure Menu* on page 78.

`CPM`

Displays the Configuration Pin Manager (CPM) level menu. For the list of commands within this menu, see *CPM Menu* on page 91.

`Device`

Displays the Device level menu. For the list of commands within this menu, see *Device Menu* on page 94.

`Disable`

Exits current menu level and returns to main root level menu. For the list of commands within the root level menu, see *Root Configuration Menu* on page 68.

`Exit`

Exit from the system.

`Filesystem`

Displays the Filesystem level menu. For the list of commands within this menu, see *Filesystem Menu* on page 96.

`Line1`

Displays the Line 1 menu for serial port 1 configuration. For more information on serial port configuration, see *Line Menu* on page *99*.

`Line2`

Displays the Line 1 menu for serial port 2 configuration. For more information on serial port configuration, see *Line Menu* on page *99*.

Line3

Displays the Line 3 menu for serial port 3 configuration. For more information on serial port configuration, see *Line Menu* on page *99*.

No clear interfaces counters

Reverts the interface counters to the last aggregate value.

No clear query port counters

Reverts the query port counters to the last aggregate value.

Nslookup

Look up host information for the given host name.

Nslookup <host>

Display host information for a specified host name.

Ping <host>

Pings the **host** destination 5 times with a 5 second timeout.

Ping <host> <count>

Pings the **host** destination the specified number (**count**) of times with a 5 second timeout.

Ping <host> <count> <timeout>

Pings the **host** destination the specified number (**count**) of times with a specified **timeout** (in seconds).

Reload

Reboots the XPort AR and reloads the configuration from Flash memory.

Reload factory defaults

Resets the XPort AR configuration to the default settings.

Show arp

Displays the ARP table

`Show history`

Displays previously entered commands.

`Show hosts`

Displays the domain settings.

`Show interfaces`

Displays network interface statistics.

`Show ip sockets`

Displays TCP and UDP state information and their associated ports.

`Show processes`

Displays thread runtime information. This command shows the list of running processes. The stack is the number of bytes used and the total stack size.

`Show query port`

Displays statistics and information on the query port.

`Show sessions`

Displays active Telnet and SSH sessions on the XPort AR.

`Show XPort`

Displays the XPort AR’s configuration.

`Trace route <host>`

Determines the path taken from a computer to a specified destination. Enter the destination IP address.

`Tunnel1`

Displays the Tunnel 1 menu for tunneling configuration. For more information on tunnel configuration, see *Tunnel Menu* on page *107*.

`Tunnel2`

Displays the Tunnel 1 menu for tunneling configuration. For more information on tunnel configuration, see *Tunnel Menu* on page *107*.

Write

Store and apply current configuration into permanent memory.

Xcr dump

Display the XML configuration to the console. For more information on XML, see *XML* on page 134.

Xcr dump <group list>

Display a specified XML configuration to the console. Separate groups with a comma. Specify group instances (if they exist) with a colon. For example:

```
> xcr dump line:1, line:2
```

Enclose groups with a white space in the name with double quotation marks. For more information on XML, see *XML* on page 134

Xcr export <file>

Save the current XPort AR's configuration to a file. Specify the name for the file; the XPort AR saves it in its root directory. For more information on XML, see *XML* on page 134.

Xcr export <file> <group list>

Save a specified XML configuration to a file. Specify the group name and the name for the file; the XPort AR saves it in its root directory. For more information on XML, see *XML* on page 134.

Xcr import <file>

Import an XML configuration onto the XPort AR. For more information on XML, see *XML* on page 134.

Xcr import <file> <group list>

Import a specific XML configuration onto the XPort AR. Specify the group and filename. For more information on XML, see *XML* on page 134.

Chem Menu

The following sections describe the configurable parameters within the Chem 1, Chem 2, Chem 3, and Chem 4 configuration menus. These commands configure email alert settings.

Auto show statistics

Continuously display email statistics.

`Cc <email address>`

Enter the email address to which the alert email is CC'ed. Separate multiple addresses with a semi-colon.

`Chem 2`

Displays the Chem 2 menu for configuration.

`Chem 3`

Displays the Chem 3 menu for configuration.

`Chem 4`

Displays the Chem 4 menu for configuration.

`Clear log`

Clears all entries from the mail log.

`Clear mail counters`

Set to zero the mail counters.

`CP send <cp group> <value>`

Specify a CP group and its value to trigger an email.

`Exit`

Exits the Chem menu and returns to the Enable menu (see *Enable Menu* on page 70).

`File <file>`

Set the path of the file to use as the email's message body.

`From <email address>`

Enter email address to display in the "From" heading of the email.

`Local port <number>`

Set local port **number** for the XPort AR to use when sending the email message.

`Local port <random>`

Set local port setting to **random** to allow the XPort AR to choose the local port.

`No cc`

Clears the CC field in the email.

`No clear mail counters`

Reverts the mail counters to the last aggregate value.

`No cp send`

Disable the CP trigger used to send the email.

`No file`

Removes the file used for the body of the email.

`No from`

Clears the “From” heading line in the email.

`No overriding domain`

Removes the overriding domain name option.

`No replyto`

Clears the Reply-To field in the email.

`No subject`

Clears the email’s Subject field.

`No to`

Clears the email’s To address field.

`Priority high`

Sets the email priority level to high. Displays as high priority if recipient’s email supports email priority settings. Corresponds to X-Priority level 2.

`Priority low`

Sets the email priority level to low. Displays as low priority if recipient’s email supports email priority settings. Corresponds to X-Priority level 4.

`Priority normal`

Sets the email priority level to normal. Corresponds to X-Priority level 3.

`Priority urgent`

Sets the email priority level to urgent. Displays as urgent priority if recipient's email supports email priority settings. Corresponds to X-Priority level 1.

`Priority very low`

Sets the email priority level to very low. Displays as very low priority if recipient's email supports email priority settings. Corresponds to X-Priority level 5.

`Replyto <email address>`

Enter the Reply-To email address. The recipient's email response is sent to this address.

`Send`

Sends the SMTP email.

Note: *Both the* ***To*** *and* ***ReplyTo*** *fields must be configured.*

`Server port <number>`

Enter the SMTP server port.

`Show`

Displays the email configuration settings.

`Show log`

Displays the email log and results of email transmissions.

`Show statistics`

Displays number of successful, unsuccessful, and in-transit emails.

`Subject <string>`

Enter the subject for the email. Spaces are not accepted.

`To <email address>`

Enter the email address to which the email alert is sent. Separate multiple addresses with a semi-colon.

`Write`

Writes the current configuration to permanent storage.

Configure Menu

The following sections describe the configurable parameters within the Configure menu.

`Arp <ip address> <mac address>`

Address Resolution Protocol (ARP) maps an IP address to a device’s MAC address. The **arp** command adds an entry to the ARP table.

`Auto show icmp`

Continuously displays ICMP state and statistics.

`Auto show ip`

Continuously displays IP statistics.

`Auto show tcp`

Continuously displays TCP statistics

`Auto show udp`

Continuously displays UDP statistics

`Clear arp-cache`

Removes all entries from the ARP table.

`Clear ftp counters`

Sets the FTP counters to zero.

`Clear host <host>`

Remove a specified entry from the DNS cache.

`Clear http counters`

Set the HTTP counters to zero.

`Clear icmp counters`

Sets the Internet Control Message Protocol (ICMP) counters to zero

Clear ip counters

Set the IP counters to zero.

Clear ip ssh counters

Set the SSH counters to zero.

Clear ip telnet counters

Set the Telnet counters to zero.

Clear rss

Clears the RSS feed data.

Clear ssh

End an active SSH session on the XPort AR.

Clear tcp counters

Set to zero the TCP counters.

Clear telnet

End an active Telnet session on the XPort AR.

Clear tftp counters

Sets the TFTP counters to zero.

Clear udp counters

Set the UDP counters to zero.

Clrscrn

Clears the screen.

Enable password

Set the password for the Enable-level menu.

Exit

Exit the Configure menu and returns to the Enable menu (see *Enable Menu* on page 70).

`Hostname <string>`

Set the system hostname.

`If 1`

Display the Interface 1 menu. For more information on serial port configuration, see *Interface 1 Level Menu* on page 88.

`Ip domain name <string>`

Set the default domain name on the XPort AR.

`Ip ftp enable`

Enable the FTP server.

`Ip ftp password <string>`

Set the administrative password for the FTP server.

`Ip ftp username <string>`

Set the administrative username for the FTP server

`IP http auth <uri> <realm>`

Create a new HTTP server authentication directive.

`IP http auth type <uri> basic`

Set an HTTP server authentication directive to the Basic Access Authentication scheme. This directive may not be secured (unless used with an external secure system) since the username and password are passed unencrypted over the network.

`IP http auth type <uri> digest`

Set an HTTP server authentication directive to the Digest Access Authentication scheme. This directive is more secure than the Basic Access Authentication scheme because the password is not sent unencrypted over the network.

`IP http auth type <uri> none`

Set the authentication type for an HTTP server authentication directive to none.

`IP http auth type <uri> ssl`

Set the authentication type for an HTTP server authentication directive to SSL.

`IP http auth type <uri> ssl-basic`

Set the authentication type for an HTTP server authentication directive to SSL-Basic.

`IP http auth type <uri> ssl-digest`

Set the authentication type for an HTTP server authentication directive to SSL-Digest.

`IP http auth user <uri> <user> <password>`

Create or modify a user for an HTTP server authentication directive.

`IP http log`

Enable HTTP server logging.

`IP http log entries <number>`

Set the maximum number of HTTP server log entries.

`IP http log format <string>`

Set the log format for the HTTP server.

`IP http max bytes <bytes>`

Set the maximum number of bytes the HTTP server accepts when receiving a request.

`IP http max timeout <seconds>`

Set the maximum timeout the HTTP server waits when receiving a request.

`IP http port <number>`

Set the port number. The HHTP server uses this port number when attempting a connection.

`IP http server`

Enable HTTP server.

`IP http ssl port <number>`

Set the SSL port number for use with the HHTP server.

`IP icmp enable`

Allow the transmission and retrieval of Internet Control Message Protocol (ICMP) packets.

`Ip name-server <ip address>`

Set the primary DNS server.

`Ip name-server <ip address> <ip address>`

Set the primary and secondary DNS servers.

`Ip ssh enable`

Enable the SSH server.

`Ip ssh port <number>`

Set the local port for SSH that the server uses.

`Ip tcp resets enable`

Sends TCP RSTs upon connection to unused ports. TCP contains six control bits, with one or more defined in each packet. RST is one of the control bits. The RST bit is responsible for telling the receiving TCP stack to immediately end a connection. Sending this flag poses a security risk.

`Ip telnet enable`

Enable and start the Telnet server.

`Ip telnet port <number>`

Set the Telnet port that the server uses.

`Ip tftp allow file creation`

Enable the automatic creation of files by the TFTP server.

`Ip tftp enable`

Enable the TFTP server.

`No arp`

Clear the ARP table.

`No clear ftp counters`

Revert the FTP counters to the last aggregate value.

`No clear ip ssh counters`

Revert the IP SSH counters to the last aggregate value.

`No clear ip telnet counters`

Reverts the IP Telnet counters to the last aggregate value.

`No clear tcp counters`

Revert the TCP counters to the last aggregate value.

`No clear tftp counters`

Revert the TFTP counters to the last aggregate value.

`No clear udp counters`

Revert the UDP counters to the last aggregate value.

`No ip domain name`

Remove the IP domain name entered (difference

`No ip ftp enable`

Disable the IP FTP.

`No ip ftp password`

Remove the FTP password

`No ip ftp username`

Remove the FTP username.

`No ip http auth <uri>`

Deletes an existing HTTP server authentication directive.

`No ip http auth user <uri> <user>`

Deletes an existing user for the specified HTTP server's authentication directive.

`No ip http auth log`

Disables HTTP server logging.

`No ip http auth log format`

Removes the log format string for the HTTP server.

`No ip http server`

Disables the HTTP server.

`No ip icmp enable`

Prevents the sending or retrieval of ICMP packets.

`No ip name-server`

Remove the name server.

`No ip ssh enable`

Disables and stops the SSH server.

`No ip tcp resets enable`

Prohibits TCP RSTs from sending on connect to unused ports.

`No ip telnet enable`

Disables the Telnet server.

`No ip tftp allow file creation`

Disables file creation via TFTP.

`No ip tftp enable`

Disables the TFTP server.

`No password`

Removes the root level password.

`No query-port enable`

Disable the query port.

`No rss enable`

Disables the RSS feed.

`No rss persistent`

Disables RSS feed data persistence.

`No snmp-server community ro`

Remove the SNMP read-only server community string.

`No snmp-server community rw`

Remove the SNMP read/write server community string

`No snmp-server contact`

Remove the SNMP server contact.

`No snmp-server description`

Clear the SNMP server description.

`No snmp-server enable`

Disable the SNMP server.

`No snmp-server enable traps`

Disables SNMP server traps.

`No snmp-server host <ip address>`

Delete the SNMP server host.

`No snmp-server host <ip address> <ip address>`

Delete the SNMP server host.

`No snmp-server location`

Clear the SNMP server location.

`No snmp-server name`

Clear the SNMP server name.

`Password`

Set the new password. Prompts for a password then requests password verification.

`Password <string>`

Enter the password on one line.

`Ppp 1`

Display the PPP menu for serial port 1. For more information on PPP configuration, see PPP Menu on page *91*.

`Ppp 2`

Display the PPP menu for serial port 2. For more information on PPP configuration, see PPP Menu on page *91*.

`Query-port enable`

Enable the query port.

`Show ftp`

Display the FTP configuration and statistics.

`Show history`

Display previously-entered commands.

`Show http`

Show the HTTP server settings.

`Show http auth`

Display the HTTP server authentication settings.

`Show http log`

Show the HTTP server log.

`Show http statistics`

Show the HTTP server settings.

`Show icmp`

Display ICMP state and statistics.

`Show ip`

Show IP statistics.

`Show rss`

Show the RSS feed settings.

`Show snmp-server`

Display SNMP server settings.

`Show ssh`

Display IP SSH configuration.

`Show telnet`

Display Telnet configuration.

`Show tftp`

Display TFTP settings and statistics.

`Show udp`

Display UDP settings and statistics

`Snmp-server community <string> ro`

Set the read-only SNMP server community.

`Snmp-server community <string> rw`

Set the read-write community within the SNMP server.

`Snmp-server contact <string>`

Set the SNMP system contact information.

`Snmp-server description <string>`

Enter description for SNMP server.

`Snmp-server enable`

Enable the SNMP server.

`Snmp-server enable traps`

Enable traps on the SNMP server.

`Snmp-server host <ip address>`

Set the primary SNMP trap host.

`Snmp-server host <ip address> <ip address>`

Set the primary and secondary SNMP trap hosts.

`Snmp-server location <string>`

Set the SNMP system location.

`Snmp-server name <string>`

Set the SNMP system name.

`Write`

Store and apply current configuration into permanent memory.

Interface 1 Level Menu

The following sections describe the configurable parameters within the Interface (IF 1) configuration menu.

`Arp timeout <number>`

Set ARP cache timeout.

`Bootp`

Enable BOOTP.

`Clear host <string>`

Removes an entry from the DNS cache.

`Clrscrn`

Clears the screen.

`Dhcp`

Enable DHCP.

`Dhcp renew`

Force DHCP to renew.

`Exit`

Exit the Interface menu and returns to the Enable menu (see *Enable Menu* on page 70).

`IP address <ip address/bits>`

Set the IP address and netmask. Enter the netmask in CIDR notation.

`IP address <ip address>`

Set the IP address.

`IP address <ip address> <ip address>`

Set the IP address and netmask. Enter the netmask in dotted notation.

`IP address filter <ip address> <ip address>`

Add a filter to the IP filter table.

`IP default-gateway <ip address>`

Set the IP address for the default gateway.

`Mac-address <mac address>`

Change the MAC address of the device.

`No bootp`

Disable BOOTP.

`No dhcp`

Disable DHCP.

`No ip address`

Remove the IP address.

`No ip address filter <ip address> <ip address>`

Remove a specified filter from the IP filter table.

`No ip default-gateway`

Remove the default gateway.

`Show`

Show interface settings.

`Show history`

Display previously-entered commands.

`Show ip address filter`

Display the IP filter table.

`Speed 10`

Set the Ethernet link to 10 Mbps (duplex is unchanged).

`Speed 10 full`

Set the Ethernet link to 10M bps (full-duplex).

`Speed 10 half`

Set the Ethernet link to 10 Mbps (half-duplex).

`Speed 100`

Set the Ethernet link to 100 Mbps (duplex is unchanged).

`Speed 100 full`

Set the Ethernet link to 100 Mbps (full-duplex).

`Speed 100 half`

Set the Ethernet link to 100 Mbps (half-duplex).

`Speed auto`

Set the Ethernet link to auto-negotiation.

`Write`

Store and apply current configuration into permanent memory.

PPP Menu

The following section describes the configurable parameters within the Point-to-Point Protocol (PPP) configuration menu. For more information on PPP, see *Point-to-Point Protocol (PPP)* on page 119.

Note: *The following section describes the parameters within the PPP 1 and PPP 2 menus.*

`Exit`

Exit the CPM menu and return to the Enable menu (see *Enable Menu* on page 70).

`Ip address <ip address> <netmask>`

Sets the local IP address and netmask.

`No ip address`

Removes the local IP address.

`No peer default ip address`

Removes the configured peer IP address.

`No ppp authentication`

Removes PPP authentication.

`No ppp enable`

Disables PPP.

`No username`

Removes the PPP authentication username and password.

`Peer default ip address <ip address>`

Sets the peer IP address.

`Ppp authentication chap`

Enables the Challenge Handshake Authentication Protocol (CHAP).

`Ppp authentication pap`

Enables the Password Authentication Protocol (PAP).

`Ppp enable`

Enables PPP.

`Show`

Displays the current PPP configuration.

`Username <username> password <password>`

Sets the PPP authentication username and password.

`Write`

Store and apply current configuration into permanent memory.

CPM Menu

The following section describes the configurable parameters within the CPM configuration menu. For more information on the CPM, see *Configuration Pin Manager* on page 131.

`Add <cp> to <group>`

Add a specified CP to a specified group.

`Add <cp> to <group> <bit>`

Add a CP to specified group at bit specified bit position.

`Clrscrn`

Clears the screen.

`Create <group>`

Creates a Configurable Pin (CP) group. The <string> is the name of the CP group.

`Delete <group>`

Remove a CP group and reset all CPs to inputs.

`Delete <cp> from <group>`

Remove a specified CP from a specified group and set it as input.

`Disable <group>`

Disable a group and make all CPs available.

`Enable <group>`

Enable a disabled CP group.

`Exit`

Exit the CPM menu and return to the Enable menu (see *Enable Menu* on page 70).

`Get <group>`

Display the value of a specified CP group.

`Set <group> <value>`

Assign a value to a specified group.

`Set <cp> as input`

Configure a CP as an assert high input.

`Set <cp> as input assert low`

Configure a CP as an assert low input.

`Set <cp> as output`

Configure a CP as an assert high output.

`Set <cp> as output assert low`

Configure a CP as an assert low output.

`Show <group>`

Show a specified CP group’s information.

`Show cp`

Show information for all Configurable Pins.

`Show groups`

Show all CP groups defined.

`Show history`

Show previously-entered commands.

`Write`

Write runtime configuration to permanent storage.

Device Menu

The following section describes the configurable parameters within the Device configuration menu.

`Clrscrn`

Clears the screen.

`CPU speed <mhz>`

Set the CPU speed.

`Dvt`

Displays the DVT menu For more information on DVT configuration, see *DVT* on page *95*.

`Exit`

Exit the Device menu and return to the Enable menu (see *Enable Menu* on page 70).

`Long name <name>`

Rename the XPort AR's long name as displayed in Command Mode and the Web Manager.

`No cpu speed`

Revert the query port counters to the last aggregate value?

`No long name`

Resets the product's long name to the default value.

`No short name`

Resets the product's short name to the default value.

Short name <name>

Set the XPort AR’s short name, displayed in Command Mode and the Web Manager. The string is a maximum 8 characters.

Show

Displays system information.

Show buffer pool

Displays information on buffer pools.

Show hardware information

Display the hardware information for the XPort AR. Shows the CPU type, CPU speed, Hardware ID, flash size, RAM size, and hard drive size.

Show history

Display previously-entered commands.

Show memory

Prompt displays:

```
This command will affect the performance of tunneling. Continue
(yes/no)?
```

Reply **yes**. System displays the following info (in both the main heap and internal buffer heap): Total memory, available memory, number of fragments, and allocated blocks.

Show XPort

Displays the XPort AR’s system information.

Write

Store and apply current configuration into permanent memory.

DVT

Note: *The DVT commands in this level will may affect the performance of the system. If tunneling is active, characters may be lost.*

Dvt all <hardware id> <host> <port>

Configure non-destructive DVT.

`Dvt eeprom`

Configure non-destructive DVT of Electrically-Erasable Programmable Read-Only Memory (EEPROM). EEPROM is a non-volatile storage chip used in computers and other devices.

`Dvt ethernet <host> <port>`

Configure non-destructive DVT for the Ethernet interface.

`Dvt hardware id <hardware id>`

Configure the DVT hardware ID.

`Dvt line <line>`

Configure nondestructive DVT of a specific line (i.e. the serial port).

`Dvt line all`

Configure nondestructive DVT for all lines (i.e. serial ports).

`Dvt ram`

Set Nondestructive DVT of RA.M

`Exit`

Exit the EVT menu and return to the Device menu (see *Device Menu* on page *94*).

Filesystem Menu

The following section describes the configurable parameters within the Filesystem menu. This level allows for the management of files in the XPort AR.

`Cat <file>`

Display the contents of a specified file.

`Cd <directory>`

Display all of the filesystem files in the current directory.

`Compact`

Compress the filesystem and frees all available space.

`Cp <source file> <destination file>`

Create a copy of an existing file. The first string parameter is the original file, the second string parameter is the name for the copied file.

`Dump <file>`

Display the contents of a specified file.

`Exit`

Exit the Filesystem menu and return to the Enable menu (see *Enable Menu* on page 70).

`Format`

Display all filesystem files and directories.

`Ls`

Display all filesystem files in the current directory.

`Ls <directory>`

Display all filesystem files in the specified directory.

`Mkdir <directory>`

Create a directory on the filesystem. The specified string is the name of the new directory.

`Mv <source file> <destination file>`

Move a file on the filesystem. The first parameter is the current file path, the second string is the new file location.

`Pwd`

Show all the filesystem files in the current directory.

`Rm <file>`

Remove a specified file from the filesystem.

`Rmdir <file>`

Remove a specified directory from the filesystem.

`Show`

Show filesystem statistics.

`Show history`

Show previously entered commands.

`Show tree`

Show all filesystem files and directories.

`Tftp get ascii <source file> <destination file> <host>`

Obtain an ASCII file using TFTP.

`Tftp get ascii <source file> <destination file> <host> <port>`

Obtain an ASCII file using TFTP.

`Tftp get binary <source file> <destination file> <host>`

Obtain a binary file using TFTP.

`Tftp get binary <source file> <destination file> <host> <port>`

Obtain a binary file using TFTP.

`Tftp put <string> <string> <string> <string>`

Send a file using TFTP.

`Tftp put ascii <source file> <destination file> <host>`

Send an ASCII file using TFTP.

`Tftp put ascii <source file> <destination file> <host> <port>`

Send an ASCII file using TFTP.

`Tftp put binary <source file> <destination file> <host>`

Send a binary file using TFTP.

`Tftp put binary <source file> <destination file> <host> <port>`

Send a binary file using TFTP.

`Touch <string>`

Create a file on the filesystem. Enter the filename to be created.

Line Menu

The following sections describe the configurable parameters within the Line 1, Line 2, and Line 3 configuration menus. These configure serial ports 1, 2, and 3.

`Auto show statistics`

Continuously display line statistics.

`Clear line counters`

Set to zero the serial counters.

`Clrscrn`

Clears the screen.

`Command mode always`

Set command mode to always enabled.

`Command mode cp`

Set Command Mode to use CP settings.

`Command mode cp <cp group> <value>`

Specify a CP group and trigger value.

`Command mode echo serial string`

Enable echoing of serial data at boot-up.

`Command mode serial string`

Set command mode to use serial settings.

`Command mode serial string <string>`

Set command mode serial string using ASCII characters.

`Command mode serial string binary <string>`

Set command mode serial string using binary values.

`Command mode signon message <string>`

Set the boot-up sign-on message using ASCII characters.

`Command mode signon message binary <string>`

Set boot-up sign-on message using binary values.

`Command mode wait time <milliseconds>`

Set boot-up wait time for CP and serial settings.

`Databits 7`

Set the XPort AR's databits to 7.

`Databits 8`

Set the XPort AR's databits to 7.

`Exit`

Exit the Line menu and return to the Enable menu (see *Enable Menu* on page 70).

`Flowcontrol hardware`

Set the flow control to hardware.

`Flowcontrol none`

Set the flow control to none.

`Flowcontrol software`

Set the flow control to software.

`No clear line counters`

Reverts the serial counters to the last aggregate value.

`Line 2`

Displays the Line 2 menu.

`Line 3`

Displays the Line 3 menu

`No command mode`

Disables command mode.

`No command mode echo`

Disables the echoing of serial data upon bootup.

`No command mode cp`

Disables the Command Mode use of CP settings.

`No command mode serial string`

Disables the Command Mode use of serial settings.

`No command mode signon message`

Removes the sign-on message displayed during Command Mode.

`No flowcontrol`

Sets the XPort AR to no flow control.

`No shutdown`

Enables the interface.

`Parity even`

Set the XPort AR's parity to even.

`Parity none`

Set the XPort AR's parity to none.

Parity odd

Set the XPort AR's parity to odd.

Show

Display the XPort AR's settings.

Show command mode

Show Command Mode settings.

Show line

Show line settings.

Show statistics

Show line statistics.

Shutdown

Disables the interface.

Speed <baud>

Set the XPort AR's speed to values between 300 and 230400.

Speed custom <baud>

Set the XPort AR's speed to values between 300 and 230400.

Stopbits 1

Set the XPort AR's stop bit to 1.

Stopbits 2

Set the XPort AR's stop bit to 1.

Tunnel 1

Displays the Tunnel 1 menu level. For more information on tunneling, see *Tunneling* on page 120.

Write

Stores and apply current configuration into permanent memory.

`Xoff <character definition>`

Sets the xoff character.

`Xon <character definition>`

Sets the xon character.

SSH Menu

The following sections describe the configurable parameters within the SSH configuration menus. For more information on SSH, see *SSH and SSL Security* on page 125.

`Client server <server>`

Set the client server RSA or DSA keys.

`Client user <user> <command>`

Set the client user, command, and RSA or DSA keys.

`Client user <user> <password> <command>`

Set the client user, password, command, and RSA or DSA keys (optional).

`Client user <user> <password> <command> <public> <private>`

Set the client user, password, command, and RSA or DSA keys.

`Client user <user> generate dsa 1024`

Generate DSA public and private keys.

`Client user <user> generate dsa 512`

Generate DSA public and private keys.

`Client user <user> generate dsa 768`

Generate DSA public and private keys.

`Client user <user> generate rsa 1024`

Generate RSA public and private keys.

`Client user <user> generate rsa 512`

Generate RSA public and private keys.

`Client user <user> generate rsa 768`

Generate RSA public and private keys.

`Clrscrn`

Clears the screen.

`Exit`

Exit the SSH menu and return to the Enable menu (see *Enable Menu* on page 70).

`Host`

Sets the RSA or DSA public (or private) keys.

`Host <key>`

Sets the RSA or DSA public (or private) key.

`Host <public> <private>`

Sets RSA (or DSA) public and private keys.

`Host generate dsa 1024`

Generate DSA public and private keys.

`Host generate dsa 512`

Generate DSA public and private keys.

`Host generate dsa 768`

Generate DSA public and private keys.

`Host generate rsa 1024`

Generate RSA public and private keys.

`Host generate rsa 512`

Generate RSA public and private keys.

`Host generate rsa 768`

Generate RSA public and private keys.

`Host user <user> <password>`

Sets the host username and password.

`Host user <user> <password> <key>`

Sets the host username, password and a public key.

`Host user <user> <password> <public> <private>`

Sets the host username, password, public keys, and private keys.

`No client server <server>`

Remove the client server.

`No client server <server> dsa`

Remove the client server DSA key.

`No client server <server> rsa`

Remove the client server RSA key.

`No client user <user>`

Remove the client user.

`No client user <user> dsa`

Remove the client user DSA key.

`No client user <user> rsa`

Remove the client user RSA key.

`No host dsa`

Removes DSA public and private keys.

`No host rsa`

Removes RSA public and private keys.

`No host user <user>`

Remove a host user.

`Show`

Show SSH settings.

`Show client server <server>`

Show client server RSA and DSA keys.

`Show client user <user>`

Show information for a client user.

`Show host dsa`

Show the full DSA public key.

`Show host rsa`

Show the full RSA public key.

`Show host user <user>`

Show information for a host user.

`Write`

Stores and apply current configuration into permanent memory.

SSL Menu

The following sections describe the configurable parameters within the SSL configuration menus. . For more information on SSL, see *SSH and SSL Security* on page 125.

`Clrscrn`

Clears the screen

`Exit`

Exit the SSL menu and return to the Enable menu (see *Enable Menu* on page 70).

`No ssl`

Removes the SSL certificate.

`Show history`

Displays previously-entered commands.

`Show ssl`

Displays the SSL certificate information.

`Ssl`

Adds a SSL certificate and private key.

`Ssl <certificate> <private>`

Adds a SSL certificate and private key.

`Ssl generate`

Generates a new self-signed SSL certificate.

`Write`

Stores and apply current configuration into permanent memory.

Tunnel Menu

The following sections describe the configurable parameters within the Tunnel configuration menu. For more information on tunneling, see *Tunneling* on page 120..

`Accept aes decryption key <string>`

Set the AES decryption key using ASCII format.

`Accept aes decryption key binary <string>`

Set the AES decryption key using binary format.

`Accept aes encryption key <string>`

Set the AES encryption key using ASCII format.

`Accept aes encryption key binary <string>`

Set the AES encryption key using binary format.

`Accept always`

Enable accept mode.

`Accept any character`

Enable accept mode upon the reception of a character.

`Accept block network`

Block the tunneling of network data.

`Accept block serial`

Block the tunneling of serial data.

`Accept cp set group <group>`

Enter the CP Group to set upon the creation or termination of a connection.

`Accept cp set group connect <value>`

Sets the CP Set Group to specified value upon connection.

`Accept cp set group disconnect <value>`

Sets the CP Set Group to specified value upon disconnection.

`Accept flush serial data`

Flush the serial data buffer upon a connection.

`Accept keep alive <milliseconds>`

Enable TCP keepalives and set the timer in milliseconds.

`Accept port <number>`

Set a specific port to use as the local port.

`Accept protocol ssh`

Use SSH for accept mode.

`Accept protocol tcp`

Use TCP for accept mode.

`Accept protocol tcp aes`

Use AES over TCP for accept mode.

`Accept protocol telnet`

Use Telnet (IAC) for accept mode.

`Accept start character`

Enable accept mode on reception of the start-character.

`Clear accept counters`

Set to zero the accept counters.

`Clear aggregate counters`

Set to zero the aggregate counters.

`Clear all counters`

Set to zero the all tunnel counters.

`Clear connect counters`

Set to zero the connect counters.

`Clrscrn`

Clears the screen

`Connect aes decryption key <string>`

Set the AES decryption key using ASCII format.

`Connect aes decryption key binary <string>`

Set the AES decryption key using binary format.

`Connect aes encryption key <string>`

Set the AES encryption key using ASCII format.

`Connect aes encryption key binary <string>`

Set AES encryption key using binary format.

`Connect always`

Enable connect mode.

`Connect any character`

Enable connect mode on reception of a character.

`Connect block network`

Block the tunneling of network data.

`Connect block serial`

Block the tunneling of serial data.

`Connect cp set group <group>`

Enter the CP Group to set upon the creation or termination of a connection.

`Connect cp set group connect <value>`

Sets the CP Set Group to specified value upon connection.

`Connect cp set group disconnect <value>`

Sets the CP Set Group to specified value upon disconnection

`Connect dsr active`

Enable connect mode if DSR is asserted.

`Connect flush serial data`

Flush the serial data buffer on a connection.

`Connect keep alive <number>`

Enable TCP keepalives and the set timer in milliseconds.

`Connect modem control active`

Enable Connect Mode when modem control pin is set to asserted.

`Connect modem emulation`

Enable modem emulation.

`Connect port <number>`

Set the specific port to use as the local port.

`Connect protocol ssh`

Use SSH for connect mode.

`Connect protocol tcp`

Use TCP for connect mode.

`Connect protocol tcp aes`

Use AES over TCP for connect mode.

`Connect protocol udp`

Use UDP for connect mode.

`Connect protocol udp aes`

Use AES over UDP for connect mode.

`Connect reconnect timer <milliseconds>`

Set the reconnect time value in milliseconds.

`Connect remote <host>`

Set the remote address in which to connect.

`Connect remote port <number>`

Set remote port.

`Connect ssh username <string>`

Set the SSH user information.

`Connect start character`

Enable connect mode on reception of the start character.

`Disconnect dsr inactive`

Enable disconnect mode to disconnect if DSR not asserted.

`Disconnect flush serial data`

Flush serial data buffer upon disconnection.

`Disconnect stop character`

Enable disconnect mode to disconnect on reception of the stop character.

`Disconnect timeout`

Enable disconnect mode to disconnect on a timeout.

`Disconnect timeout <number>`

Set disconnect mode timeout in milliseconds.

`Echo start character`

Enable forwarding (tunneling) of the start character.

`Echo stop character`

Enable forwarding (tunneling) of stop-character.

`Exit`

Exit the Tunnel menu and return to the Enable menu (see *Enable Menu* on page 70).

`Kill accept connection`

Kill the active accept mode connection.

`Kill connect connection`

Kill the active connect mode connection.

`Line 1`

Displays the Line 1 menu option (see *Line Menu* on page 99).

`Modem connect string <string>`

Add to the connect string in modem emulation

`Modem connect string <string>`

Add to the connect string in modem emulation.

`Modem echo commands`

Echo modem commands.

`Modem echo pluses`

Echo +++ when entering modem command mode.

`Modem error unknown commands`

Returns an error upon unknown AT commands.

`Modem numeric response codes`

Use numeric response codes.

`Modem text response codes`

Use text-based response codes.

`Modem verbose`

Use verbose status codes

`No accept`

Disable accept mode.

`No accept aes decryption key`

Remove the AES decryption key.

`No accept aes key encrypt`

Remove the AES encryption key.

`No accept block network`

Forward (tunnel) network data.

`No accept block serial`

Forward (tunnel) serial data.

`No accept cp set group`

Removes the CP Set Group.

`No accept flush serial data`

Do not flush serial data buffer on connection.

`No accept keep alive`

Disable TCP keepalives.

`No accept port`

Use a random port number as the local port.

`No clear accept counters`

Unzeros accept counters.

`No clear aggregate counters`

Unzeros aggregate counters.

`No clear all counters`

Unzeros all tunnel counters.

`No clear connect counters`

Unzeros connect counters.

`No connect`

Disable connect mode.

`No connect aes decryption key`

Remove the AES decryption key.

`No connect aes encryption key`

Remove the AES encryption key.

`No connect block network`

Forward (tunnel) network data.

`No connect block serial`

Forward (tunnel) serial data.

`No connect cp set group`

Removes the CP Set Group.

`No connect flush serial data`

Do not flush serial data buffer on connection.

`No connect keep alive`

Disable TCP keepalives.

`No connect port`

Use a random port number as the local port.

`No connect remote address`

Remove remote address to connect to.

`No connect remote port`

Remove remote port to connect to.

`No connect ssh username`

No SSH user specified.

`No disconnect`

Disable disconnect mode.

`No disconnect flush serial data`

Do not flush serial data buffer on disconnection.

`No echo start character`

Disable forwarding (tunneling) of start-character.

`No echo stop character`

Disable forwarding (tunneling) of stop-character.

`No modem connect string`

Remove optional CONNECT string information.

`No modem echo commands`

Do not echo modem commands.

`No modem echo pluses`

Do not echo +++ when entering modem command mode.

`No modem verbose`

Use decimal status codes.

`No packing mode`

Disable packing mode.

`No packing send character`

Remove the send character.

`No packing trailing character`

Remove the trailing character.

`No serial buffer size`

Set buffers used in tunneling of data to the default.

`No serial wait for read timeout`

Disable waiting for read timeout before returning serial data.

`No start character`

Remove the start character.

`No stop character`

Remove the stop character.

`Packing mode send character`

Enable packing mode to pack data and transmit upon the send character.

`Packing mode timeout`

Enable packing mode to pack data and transmit using a timeout.

`Packing send character <string>`

Set the send character (string format: C, HEX: 0x##, Decimal: ###).

`Packing threshold <bytes>`

Set the threshold (byte count).

`Packing timeout <milliseconds>`

Set the timeout value in milliseconds.

`Packing trailing character <string>`

Set the trailing character.

`Serial buffer size <bytes>`

Set the size of the buffers to using in tunneling of data.

`Serial read timeout <milliseconds>`

Set the time in milliseconds to wait for serial data.

`Serial wait for read timeout <milliseconds>`

Make tunneling wait for read timeout before returning serial data.

`Show`

Show tunneling configuration.

`Show history`

Show previously-entered commands.

`Show statistics`

Show connection statistics.

`Start character <string>`

Set the start character (string format: C, HEX: 0x##, Decimal: ###).

`Stop character <string>`

Set the stop- character (string format: C, HEX: 0x##, Decimal: ###).

`Tunnel 2`

Displays the Tunnel 2 menu option.

Write

Stores and apply current configuration into permanent memory.

6: Point-to-Point Protocol (PPP)

Point-to-Point Protocol (PPP) establishes a direct connection between two nodes. It defines a method for data link connectivity between devices using physical layers (such as serial lines). Some of the PPP features include: error detection, compression, and authentication. For each of these capabilities, PPP has a separate protocol.

The XPort AR supports two types of PPP authorization: Password Authentication Protocol (PAP) and Challenge Handshake Protocol (CHAP). Both of these authentication methods require the configuration of a username and password. It also supports no authentication scheme when no authentication is required during link negotiation.

PAP is an authentication protocol in PPP. It offers a straightforward method for the peer to determine its identity. Upon the link establishment, the user ID and password are repeatedly sent to the authenticator until it is acknowledged or the connection is terminated.

Note: *PAP is not a strong authentication process. There is no protection against trial-and-error attacks. As well, the peer is responsible for the frequency of the communication attempts*.

CHAP is a more secure method than PAP. It works by sending a challenge message to the connection requestor. Using a one-way hash function, the requestor responds with its value. If the value matches the server's own calculations, authentication is provided. Otherwise, the connection is terminated.

Note: *RFC1334 defines both CHAP and PAP.*

Use the XPort AR's Web Manager or CLI to configure a network link using PPP over a serial line. Turn off Connect Mode, Accept Mode, and Command mode before enabling PPP.

The XPort AR acts as the server side of the PPP link; it can require authentication and assign an IP address to the peer. Upon PPP configuration, IP packets are routed between Ethernet and PPP interfaces.

7: Tunneling

Serial tunneling allows for devices to communicate over a network, without the realization of other devices connecting between them. Tunneling parameters are configured using the Web Manager's *Tunnel 1 and Tunnel 2 Settings* (on page 28) or Command Mode's *Tunnel Menu* (on page 107).

The XPort AR supports 2 tunneling connections simultaneously per serial port. One of these connections is Connect Mode, the other connection is Accept Mode. The connections on one serial port are separate from those on the other serial port.

- Connect Mode: the XPort AR actively makes a connection. The receiving node on the network must listen for the Connect Mode's connection. Connect Mode is disabled by default.
- Accept Mode: the XPort AR listens for a connection. A node on the network initiates the connection. Accept Mode is enabled by default.
- Disconnect Mode: this mode defines how an open connection stops the forwarding of data. The specific parameters to stop the connection are configurable. Once the XPort AR's Disconnect Mode observes the defined event occur, it will disconnect both Accept Mode and Connect Mode connections on that port.

When any character comes in through the serial port, it gets copied to both the Connect Mode connection and the Accept Mode connection (if both are active).

Connect Mode

For Connect Mode to function, it must be enabled, have a remote station (node) configured, and a remote port configured (TCP or UDP). When enabled, Connect Mode is always on.

Enter the remote station as an IP address or DNS name. The XPort AR will not make a connection unless it can resolve the address. For DNS names, after 4 hours of an active connection, the XPort AR will re-evaluate the address. If it is a different address, it will close the connection.

Connect Mode supports the following protocols:

- TCP
- AES encryption over UDP
- AES encryption over TCP
- SSH (the XPort AR is the SSH client)
- UDP (available only in Connect Mode since it is a connectionless protocol).

When setting AES encryption, both the encrypt key and the decrypt key must be specified. The encrypt key is used for data sent out. The decrypt key is used for receiving data. Both of the keys may be set to the same value.

For Connect Mode using UDP, if the remote address or port is not configured, then the XPort AR accepts packets from any device on the network. It will send packets to the last device that sent it packets. As a result, it is advised to configure the remote address and port. When the remote port and station are configured, the XPort AR ignores date from other sources.

Note: *The Local Port in Connect Mode is not the same port configured in Accept Mode.*

To ignore data sent to the XPort AR, enable the blocking of serial data or network data (or both).

The TCP keepalive time is the time in which probes are periodically sent to the other end of the connection. This ensures the other side is still connected.

To configure SSH, the SSH client username must be configured. In Connect Mode, the XPort AR is the SSH client. Ensure the XPort AR's SSH client username is configured on the SSH server before using it with the XPort AR.

Connect Mode has five states:

- Disabled (no connection)
- Enabled (always makes a connection)
- Active if it sees any character from the serial port
- Active if it sees a specific (configurable) character from the serial port
- Modem emulation

For the “any character” or “specific character” connection states, the XPort AR waits and retries the connection if the connection cannot be made. Once it makes a connection and then disconnects, it will not reconnect until it sees any character or the start character again (depending on the configured setting).

Configure the Modem Control Active setting (for DSR or DTR) to start a Connect Mode connection when the signal is asserted. The XPort AR will indefinitely try to make a connection forever. If the connection closes, it will not make another connection unless the signal is asserted again.

Accept Mode

In Accept Mode, the XPort AR waits for a connection. The configurable local port is the port the remote device connects to for this connection. There is no remote port or address. The default local port is 10001 for serial port 1 and 10002 for serial port 2.

Accept Mode supports the following protocols:

- SSH (the XPort AR is the server in Accept Mode). When using this protocol, the SSH server host keys and at least one SSH authorized user must be configured.
- TCP
- AES encryption over TCP

- Telnet/IAC mode (The XPort AR currently supports IAC codes. It drops the IAC codes when telnetting and does not forward them to the serial port).

Accept Mode has the following states:

- Disabled (close the connection)
- Enabled (always listening for a connection)
- Active if it receives any character from the serial port
- Active if it receives a specific (configurable) character from the serial port (same start character as Connect Mode's start character)
- Modem control signal

Disconnect Mode

Disconnect Mode ends Accept Mode and Connect Mode connections. When disconnecting, the XPort AR shuts down connections gracefully.

The following 3 settings end a connection:

- The XPort AR receives the stop character.
- The timeout period has elapsed and no activity is going in or out of the XPort AR. Both Accept Mode and Connect Mode must be idle for the time frame.
- The XPort AR observes the modem control inactive setting.

To clear data out of the serial buffers upon a disconnect, configure buffer flushing.

Packing Mode

Packing Mode takes data from the serial port, groups it together, and sends it out to nodes on the network. The groupings may be configured by size or by time intervals.

The following settings are configurable for Packing Mode:

- Disable Packing Mode
- The Packing Mode timeout. The data is packed for a specified period of time before being sent out.
- The Packing Mode threshold. When the buffer fills to a specified amount of data (and the timeout has not elapsed), the XPort AR packs the data and sends it out.
- The send character. Similar to a start or stop character, the XPort AR packs the data until it sees the send character. The XPort AR then sends the packed data and the send character in the packet.
- A trailing character. If a trailing character is defined, this character is appended to data put on the network immediately following the send character.

Modem Emulation

The XPort AR supports Modem Emulation mode for devices that send out modem signals. There are two different modes supported:

Command Mode: sends back verbal response codes.

Data Mode: information transferred in is also transferred out.

It is possible to change the default on bootup for verbose response codes, echo commands, and quiet mode. The current settings can be overridden, however on bootup it will go back to the programmed settings.

Configure the connect string as necessary. The connect string appends to the communication packet when the modem connects to a remote location. It is possible to append additional text to the connect message.

Command Mode

The Modem Emulation's Command Mode supports the standard AT command set. For a list of available commands from the serial or telnet login, enter **AT?**. Use **ATDT**, **ATD**, and **ATDP** to establish a connection:

+++	Switches to command mode if entered from serial port during connection.
AT?	Help.
ATDT<Address Info>	Establishes the TCP connection to socket (<IP>/<port>).
ATDP<Address Info>	See ATDT.
ATD	Like ATDT. Dials default connect mode remote address and port.
ATO	Switches to data mode if connection still exists. Vice versa to '+++'.
ATEn	Switches echo in command mode (off - 0, on - 1).
ATH	Disconnects the network session.
ATI	Displays modem information.
ATQn	Quiet mode (0 - enable results code, 1 - disable results code.)
ATVn	Verbose mode (0 - numeric result codes, 1 - text result codes.)
ATZ	Restores the current state from the setup settings.
A/	Repeat last valid command.

All of these commands behave like a modem. For commands that are valid but not applicable to the XPort AR, an "OK" message is sent (but the command is silently ignored).

The XPort AR attempts to make a Command Mode connection as per the IP/DNS/port numbers defined in Connect Mode. It is possible to override the remote address, as well as the remote port number.

Note: Configure either the IP address using the address on its own (<xxx.xxx.xxx.xxx>), or the IP address and port number by entering <xxx.xxx.xxx.xxx>:<port> . The port number cannot be entered on its own.

For ATDT and ATDP commands less than 255 characters, the XPort AR replaces the last segment of the IP address with the configured Connect Mode remote station address. It is possible to also use the last two segments if they're under 255 characters. For example, if the address is 100.255.15.5, entering "ATDT 16.6" results in 100.255.16.6.

When using ATDT and ATDP, enter 0.0.0.0 to switch to Command Mode. Once Command Mode is exited, the XPort AR reverts back to modem emulation mode.

By default, the +++ characters are not passed through the connection. Turn on this capability using the **modem echo plus** command.

Serial Line Settings

Serial line settings are configurable for both serial line 1 and serial line 2.

Configure the buffer size to change the maximum amount of data the serial port stores. For any active connection, the XPort AR sends the data in the buffer. The read timeout is used for periodically sending data. If the buffer is not full (i.e. reached the buffer size) but the read timeout time has elapsed, the data in the buffer is sent out.

Statistics

The XPort AR logs statistics for tunneling. The **Dropped** statistic displays connections ended by the remote location. The **Disconnected** statistic displays connections ended by the XPort AR.

8: SSH and SSL Security

The XPort AR supports Secure Shell (SSH) and Secure Sockets Layer (SSL). These security protocols are configurable through the Web Manager (see *SSH Settings* on page 42 and *SSL Settings* on page 46) and Command Mode (see *SSH Menu* on page 103 and *SSL Menu* on page 106).

Note: *This chapter overviews security configuration using Web Manager.*

Secure Shell: SSH

SSH is a network protocol for securely accessing a remote device. This protocol provides a secure, encrypted communication channel between two hosts over a network.

To configure the SSH settings, there are two instances that require configuration: when the XPort AR is the SSH server and when it is an SSH client. The SSH server is used by the CLI (Command Mode) and for tunneling in Accept Mode. Use the SSH client for tunneling in Connect Mode.

SSH Server Configuration

To configure the XPort AR as an SSH server, there are two requirements:

- Defined host keys: both private and public keys are required. They keys are used for the Diffie-Hellman key exchange (used for the underlying encryption protocol).
- Defined users: these users are permitted to connect to the XPort AR's SSH server.

To configure SSH server settings:

1. Click **SSH → Server Host Keys** from the navigation menu. The SSH Server: Host Keys page displays.
2. To configure the host keys:

   a) If the keys exist, locate the **Private Key** and **Public Key** using the **Browse** button. Select the **Key Type** (**RSA** is more secure) and click **Submit** to upload the keys.

      i. SSH keys may be created on another computer and uploaded to the XPort AR. To do so, use the following command using Open SSH to care a 768-bit DSA key pair:

      ```
      ssh-keygen –b 768 –t dsa
      ```

b) If the keys do not exist, select the **Key Type** and the key's **Bit Size** from the **Create New Keys** section. Click **Submit** to create new private and public host keys.

Note: Generating new keys with a large bit size results in very long key generation time.

3. Click **SSH → Server Auth Users** from the navigation menu. The SSH Server: Authorized Users page displays.

4. Enter the **Username** and **Password** for authorized users.

5. If available: locate the **Public RSA Key** or the **Public DSA Key** by clicking **Browse**. Configuring a public key results in public key authentication; this bypasses password queries.

Note: When uploading the certificate and the private key, ensure the private key is not compromised in transit.

SSH Client Configuration

To configure the XPort AR as an SSH client, there is one requirement:

- An SSH client user is configured and exists on the remote SSH server.

To configure SSH client settings:

1. Click **SSH → Client Users** from the navigation menu. The SSH Client: Users page displays.

2. (Required) Enter the **Username** and **Password** to authenticate with the SSH server.

3. (Optional) Complete the SSH client user information as necessary. The **Private Key** and **Public Key** automate the authentication process; when configured and the user public key is known on the remote SSH server, the SSH server does not require a password. (Alternatively, generate new keys using the **Create New Keys** section.). The **Remote Command** is provided to the SSH server. It specifies the application to execute upon connection. The default is a command shell.

Note: Configuring the SSH client's known hosts is optional. It prevents Man-In-The-Middle (MITM) attacks.

Secure Sockets Layer: SSL

SSL uses cryptography to offer authentication and privacy to message transmission over the Internet. Typically, only the server is authenticated. SSL allows the communication of client/server applications without eavesdropping and message tampering. SSL uses the public-and-private key encryption system from RSA, which also includes the use of a digital certificate.

SSL runs on layers between application protocols (HTTP, SMTP, etc.) and the TCP transport protocol. It is most commonly used with HTTP (thus forming HTTPS).

On the XPort AR, configure an SSL certificate for the HTTP server to listen on the HTTPS port. This certificate can be created elsewhere and uploaded to the device.

Alternatively, it can be automatically generated on the device; this certificate type is a self-signed certificate.

Note: *When uploading the certificate and the private key, ensure the private key is not compromised in transit.*

To upload a new certificate, see *Upload Certificate* on page 46. To create a new self-signed certificate, see *Create New Self-Signed Certificate* on page 47.

9: Using Email

The XPort AR has a Simple Mail Transfer Protocol (SMTP) client. SMTP is a TCP/IP protocol used in sending and receiving email. Its objective is to send email efficiently and reliably.

There are three ways to send an email from the XPort AR:

1. Via the Web Manager (See *Configuration Using Web Manager* on page 17).
2. Via Command Mode by using the Send command (See *Configuration Using Telnet or Serial Port* on page 66).
3. By configuring a CP or a CP group (See *Configuration Pin Manager* on page 131). When the CP or the CP group changes state to the pre-specified value, an email alert is sent.

SMTP Configuration

This section covers email configuration using Command Mode. (See *Configuration Using Telnet or Serial Port* on page 66.)

The minimum requirements for SMTP configuration are:

- At least one address configured for the “To” field or “Cc” field.
- The “From” address field configured.

Note: *A “Reply-To” field is also available for configuration. This differs from the “From” field in that all replies from the recipient will be sent to this address.*

When configuring the “To” and “Cc” fields, separate multiple addresses with a semi-colon (;).

The email queue separates email addresses by domain. One email is sent per domain (not per email address). The XPort AR makes a connection directly to the destination SMTP server instead of a relay server. This prevents the message from not reaching the recipient because of spam filters.

Use the **`File`** command for the body of the email’s text. The email’s text must be saved in a file; configure the location of this message file. The XPort AR permits entering a filepath even if the file itself is not created yet. If the file does not exist when the email is sent, the body of the email reads “file does not exist”.

Priority Levels

The default priority level for the XPort AR's emails is Normal priority. The XPort AR has 5 configurable priority levels; certain recipient systems have filters based on these priority levels.

Configurable priority levels are:

Priority	**XPriority Level**
Urgent	1
High	2
Normal (default)	3
Low	4
Very Low	5

Some email programs may translate an Urgent priority to High, and Very Low priority to Low.

The XPort AR makes an SMTP connection to a destination server. By default, it connect to the destination's port 25. Override this port number by using the **`Server Port`** command.

DNS Records

Domain Name Service (DNS) translates text-based domain names to the numeric IP addresses necessary for locating the domain's server on the Internet. Many DNS servers have multiple records per domain. To resolve these addresses, the XPort AR's DNS server listing looks for MX records first. MX is the Mail Exchange Record; it is an entry in the domain name table identifying the mail server responsible for managing emails for that domain name.

If the MX record is not available, then the DNS server uses the default record. If it cannot find the default record, it will not send the email.

Extended Hello

When the XPort AR makes a connection to the recipient's SMTP server, it send an EHLO message. This message contains the XPort AR's domain.

Use the **`Overriding Domain`** command to change the domain provided in the EHLO message.

For a more information EHLO, see RFC 2821.

Email Statistics

Use the "Show Statistics" command to display the XPort AR's email statistics.

Use the “Show Log” command to display the email log. When the system sends an email, the following information is logged:

1. Messages the XPort AR sends to the SMTP server.
2. Messages from the SMTP server to the XPort AR.
3. SMTP commands and replies.

Note: *The XPort AR does not log email message contents.*

10: Configuration Pin Manager

There are 11 configurable pins on the XPort AR. All CPs (except for 5) are shared by some other function on the XPort AR. Some of the CPs are assigned to serial port 1 (dtr/dsr for modem control and rts/cts for hardware flow control), others to serial port 2 (dtr/dsr for modem control, rts/cts for hardware flow control, and tx/rx groups as well).

CPs are configurable individually, or may be clustered together and configured as a single group (CP group). This increases flexibility when incorporating the XPort AR into another system.

Each CP group is a 32 bit variable. When a CP is added to a CP group, it is assigned to a bit position within the group. A CP cannot be assigned to a group until it is configured. A CP can be a member of multiple groups, but may only be active in one.

The Configurable Pin Manager (CPM) is available through the Web Manager (see *Configuration Using Web Manager* on page 17) or through Command Mode (see *Configuration Using Telnet or Serial Port* on page 66).

Configurable Pins

To view a CP's configuration:

1. If using the Web Manager:
   a) Click **CPM → CPs** from the navigation menu. The CPM: Configurable Pin window displays.
   b) Click the specific **CP** from the Current Configuration table. The CP's configuration displays in the CP Status table.
2. If using Command Mode (the CLI):
   a) Enter Enable → CPM to access the CPM level menu.
   b) Type **show cp**.
3. The CP table displays the following:

CP	Indicates the Configurable Pin number.
Pin #	Indicates the hardware pin number associated with the CP.
Configured As	Displays the CPs configuration. A CP configured as **Input** is set to read input. A CP configured as **Output** drives data out of the XPort AR. **Peripheral** is a setting assigned by the XPort AR.

State	A value of **1** means asserted. **0** means de-asserted. **I** indicates the CP is inverted.
Groups	Indicates the number of groups in which the CP is a member.
Active In Group	A CP can be a member of several groups. However, it may only be active in one group. This field displays the group in which the CP is active.

CP Groups

To view a CP group's configuration:

1. If using the Web Manager:

   a) Click **CPM → Groups** from the navigation menu. The CPM: Groups window displays.

   b) Click the CP groups from the Current Configuration table. The CP's configuration displays in the Group Status table.

2. If using Command Mode (the CLI):

   a) Enter Enable → CPM to access the CPM level menu.

   b) Type **show group <name>**.

3. The Group Status table displays the following:

Name	Displays the CP number.
State	Current enable state of the CP. *Note: Peripheral pins are locked.*
Value	Displays the last bit in the CP's current value.
Bit	Visual display of the 32 bit placeholders for a CP.
I/O	A "+" symbol indicates the CP is asserted (the voltage is high). A "-" indicates the CP voltage is low.
Logic	An "I" indicates the CP is inverted.
State	Displays the assertion value of the corresponding bit.
CP#	Displays the CP number.
Groups	Lists the groups in which the CP is a member.

The CP group table displays the CPs assigned to it. It also displays the CP's bit position within the CP group. The wave form shows the actual voltage of inputs and outputs (a value of 1 indicates a high voltage). The state shows the assertion level.

To configure a group's value:

1. If using the Web Manager:

   a) Click **CPM → Groups** from the navigation menu. The CPM Groups window displays

   b) To create a CP group:

i. Enter a group name in the **Create Group** field.

ii. Click **Submit**. Changes are applied immediately to the XPort AR.

c) To delete a CP group:

i. Select the CP group from the **Delete Group** drop-down list.

ii. Click **Submit**. Changes are applied immediately to the XPort AR.

d) To enable or disable a CP group:

i. Select the CP group from the **Set** drop-down list.

ii. Select the state (**Enabled** or **Disabled**) from the drop-down list.

iii. Click **Submit**. Changes are applied immediately to the XPort AR.

e) To set a CP group's value:

i. Select the CP group from the **Set** drop-down list.

ii. Enter the CP group's value in the **value** field.

iii. Click **Submit**. Changes are applied immediately to the XPort AR.

f) To add CP to a CP group:

i. Select the CP from the **Add** drop-down list.

ii. Select the CP group from the drop-down list.

iii. Select the CP's bit location from the **bit** drop-down menu.

iv. Click **Submit**. Changes are applied immediately to the XPort AR.

g) To delete a CP from a CP group:

i. Select the CP from the **Remove** drop-down list.

ii. Select the CP group from the drop-down list.

iii. Click **Submit**. Changes are applied immediately to the XPort AR.

2. If using Command Mode:

a) Type **`enable`** → **`cpm`** to access the CPM level menu.

b) Use the add, delete, and set commands to configure values within Command Mode (for more information on these parameters, see *PPP Menu* on page 91).

Note: *Each CP with a bit position value of 1 (when the decimal value is converted to binary) has an asserted state.*

11: XML

The XPort AR supports configuration using Extensible Markup Language (XML). XML's main purpose is to assist the transmission of data across different systems.

Two things are required for XML:

- It must be well-formed. The XML structure must adhere to general XML format rules.
- It must be valid. It must comply with the XML schema.

Every command that is executable from the XPort AR's Command Mode is available for configuration by XML (however, some of the commands are grouped differently). To configure a unit by XML, configure an XPort AR. Export all or part of the settings (called groups) to be applied to other units. Import the saved configuration onto other XPort AR units as necessary (this reduces the need for manual configuration of each unit).

Note: *If there are any errors in the XML configuration, the XPort AR will reject the entire configuration. Also, passwords, private keys, and certificates are not imported for security reasons.*

Use XML to configure the device by exporting the current configuration as an XML file using the CLI, the filesystem, the Web Manager, or FTP. These methods are also used when importing a configuration onto a device. The complete or partial configuration may be exported or imported onto the XPort AR.

XML Configuration Record Schema

XML Configuration Records (XCRs) are exported using the following DTD:

```
<!DOCTYPE configrecord [
<!ELEMENT configrecord (configgroup+)>
<!ELEMENT configgroup (configitem+)>
<!ELEMENT configitem (value+)>
<!ELEMENT value (#PCDATA)>
<!ATTLIST configrecord version CDATA #IMPLIED>
<!ATTLIST configgroup name CDATA #IMPLIED>
<!ATTLIST configgroup instance CDATA #IMPLIED>
<!ATTLIST configitem name CDATA #IMPLIED>
<!ATTLIST value name CDATA #IMPLIED>
]>
```

The XPort AR’s schema (or template), is structured as following:

The ELEMENT tag

- The XML document element is known as a <configrecord>; this is the root element.
- Within each <configrecord> are the configuration groups, contained within the <configgroup> element. A <configrecord> must have one or more <configgroup> element. The configuration group takes “name” and “instance” attributes.

  Note: *The items within the <config group> are the groups listed within the Web Manager groups. See XML Configuration on page 52.*
- Within each configuration group are configuration items, contained within the <configitem> element. Each configuration group must have one or more configuration items. The configuration item is a specific grouping of configurable parameters relevant to the parent group. It accepts the “name” attribute.
- A <configitem> must have at least one <value>. This element specifies the actual value of the configuration parameter. It accepts the “name” attribute.

  Note: *In general, an empty <value> clears the value to its default setting.*
- A <value> element contains the configuration value.

The ATTLIST tag

- Each <configrecord> tag can have an optional “version” attribute.
- Each <configgroup> tag can have both (or one) “name” and “instance” as optional attributes.
- Each <configitem> tag can have “name” as an attribute.
- Each <value> tag can have “name” as an attribute.

Attributes

- Use the “name” attribute to identify a group, item, or value. It is always a quoted string.
- Use the “instance” attribute to identify the specific option (such as the serial port number). It is always a quoted string.

Figure 11-1. XML Group Example

```
<?xml version=”1.0” standalone=”yes”?>
<configrecord>
   <configgroup name = “serial command mode” instance = “1”>
       <configitem name = “mode serial string”>
              <value>disable</value>
       </configitem>
   </configgroup>
</configrecord>
```

Figure 11-2. XML Example With Multiple Named Values

```
<?xml version=”1.0” standalone=”yes”?>
<configgroup name = "ssh server">
       <configitem name = "host rsa keys">
           <value name = "public key"></value>
           <value name = "private key"></value>
       </configitem>
   </configgroup>
```

Figure 11-3. XML Example With Multiple Items

```
<?xml version=”1.0” standalone=”yes”?>
<configgroup name = "email" instance = "1">
       <configitem name = "to">
           <value>john.doe@somewhere.com</value>
       </configitem>
       <configitem name = "from">
           <value>evolution@xportar.com</value>
       </configitem>
   </configgroup>
```

Figure 11-4. XML Example With Multiple Groups

```
<?xml version=”1.0” standalone=”yes”?>
<configgroup name = "ftp server">
       <configitem name = "state">
           <value>enable</value>
       </configitem>
       <configitem name = "admin username">
           <value>admin</value>
       </configitem>
       <configitem name = "admin password">
           <value><!-- configured and ignored --></value>
       </configitem>
   </configgroup>
   <configgroup name = "tftp server">
       <configitem name = "state">
           <value>enable</value>
       </configitem>
       <configitem name = "allow file creation">
           <value>disable</value>
       </configitem>
   </configgroup>
```

***Note:** The above example also displays the "configured and ignored" password; this indicates the password exists but will not be used in an XML import.*

Configuration using XML

There are several methods for configuring the XPort AR using XML. The following section overviews this process using the Web Manager, Command Mode, or FTP.

Configure an XPort AR with XML using the following steps:

1. Configure an XPort AR with the desired settings using the Web Manager (see *Configuration Using Web Manager* on page 17) or the Command Mode (see *Configuration Using Telnet or Serial Port* on page 66).
2. Export all of the settings or part of the settings of the configured XPort AR using one of the following methods:

   a) Using the Web Manager, select the groups to export from the XML page (see *XML Configuration* on page 52). If no group is selected, all groups will be exported. When the filesystem is used, note the location of the file (as specified in the text box).

   b) Using Command Mode, enter the groups to export using the **xcr** command (see *Enable Menu* on page 70). The method used to access the CLI (serial port, SSH, or Telnet) does not impact the XML configuration.

   c) Using FTP, log into the XPort AR. Download the “xport_ar.xml” file containing the configuration. The configuration is generated dynamically.

   Note: *The instance is required when exporting groups.*
3. Connect the unconfigured XPort AR and locate it on the network.
4. Import all or part of the configuration settings onto the XPort AR using one of the following methods:

   a) Using the Web Manager, select the groups to import and apply to the XPort AR (see *XML Configuration* on page 52).

   b) Using Command mode, apply an XML configuration by pasting the XML file contents into the CLI session at any time. Importing a configuration via the CLI may be done at any level, including the root.

   c) Using FTP, log into the XPort AR. Upload the “xport_ar.xml” file. The configuration is immediately processed. Nothing is stored on the filesystem.

   The XPort AR is now configured using the same configuration as the original XPort AR. Repeat steps 3 and 4 for all XPort ARs requiring this configuration.

   The Reboot group allows for the device to be rebooted after an XML change. Change its value from **disable** to **enable** to automatically reboot the XPort AR after an XML configuration import.

XML Groups

The following is the list of the groups available for importing and exporting on the XPort AR. To view the contents of the export groups, use the Web Manager’s **Export XCR data to browser** feature, described on page 52).

Import-Only Groups

When configuring the XML schema to import to an XPort AR, there are additional configurations that may be added that are not available when exporting. For example, the Reboot group (which causes the XPort AR to reboot) is not a configurable setting that can be exported. However, it may be added to an XML schema manually to ensure the XPort AR reboots after applying the XML configuration. These are labeled as Import in the Import/Export column in the following table:

Table 11-1. XPort AR Import and Export Groups

Group Name	Item Name	Value Name	Value	Import/Export	Additional Information
reboot	state		enable	Import	Force the XPort AR to reboot after processing.
			disable	Import	
restore factory defaults	state		enable	Import	Before processing, reset the XPort AR to factory defaults.
			disable	Import	
interface	bootp state		enable	Import and Export	
			disable	Import and Export	
	dhcp state		enable	Import and Export	
			disable	Import and Export	
	dhcp client id			Import and Export	Set the identity of the client device.
	mac address			Import and Export	Specify the MAC address of the Ethernet card.
	domain			Import and Export	
	hostname			Import and Export	
	ip address			Import and Export	
	network mask			Import and Export	
	default gateway			Import and Export	
	primary dns			Import and Export	
interface	secondary dns			Import and Export	
ethernet	auto negotiate		enable	Import and Export	If set to **enable**, auto-negotiation is used to determine the link speed and duplex. If not set to **enable**, the speed and duplex items are exported.
			disable	Import and Export	
	speed		10	Import and Export	Specify the speed on the Ethernet connection (10 or 100). Only valid if auto-negotiation is not enabled.

Group Name	Item Name	Value Name	Value	Import/Export	Additional Information
			100	Import and Export	Specify the speed on the Ethernet connection (10 or 100). Only valid if auto-negotiation is not enabled.
	duplex		half	Import and Export	Specify the duplex of the Ethernet connection. Only valid if auto-negotiation is not enabled.
			full	Import and Export	Specify the duplex of the Ethernet connection. Only valid if auto-negotiation is not enabled.
command mode password	system			Import and Export	Set the password for the system (root) level of the CLI.
	enable			Import and Export	Sets the password for the enable level of the CLI.
email	to			Import and Export	Multiple to addresses may be separated with semicolons or input as separate “to” items.
	from			Import and Export	
	reply to			Import and Export	
	cc			Import and Export	Multiple cc address may be separated with semicolons or input as separate “cc” items.
	subject			Import and Export	
	message file			Import and Export	
	local port			Import and Export	
	server port			Import and Export	
	priority		Very Low	Import and Export	
			Low	Import and Export	
			Normal	Import and Export	
			High	Import and Export	
			Urgent	Import and Export	
	overriding domain			Import and Export	
	cp	group		Import and Export	
		trigger value		Import and Export	

Group Name	Item Name	Value Name	Value	Import/Export	Additional Information
line	state		enable	Import and Export	
			disable	Import and Export	
	baud rate			Import and Export	Any value from 300 to 230400.
	data bits		7	Import and Export	
			8	Import and Export	
	parity		none	Import and Export	
			even	Import and Export	
			odd	Import and Export	
	stop bits		1	Import and Export	
			2	Import and Export	
	flow control		hardware	Import and Export	
			software	Import and Export	
			none	Import and Export	
	xon char			Import and Export	Set the x-on character. Enter as a hexadecimal byte.
	xoff char			Import and Export	Set the x-off character. Enter as a hexadecimal byte.
ftp server	state		enable	Import and Export	
			disable	Import and Export	
	admin username			Import and Export	
	admin password			Import and Export	
tftp server	state		enable	Import and Export	
			disable	Import and Export	
	allow file creation			Import and Export	
arp	arp timeout			Import and Export	
	arp entry	ip address		Import	Add a dynamic entry to the ARP table.
		mac address		Import	

Group Name	Item Name	Value Name	Value	Import/Export	Additional Information
	arp delete			Import	Remove an entry from the ARP table. Specify the entry by its IP address.
snmp	state		enable	Import and Export	
			disable	Import and Export	
	system name			Import and Export	
	system contact			Import and Export	
	system location			Import and Export	
	traps	state	enable	Import and Export	
			disable	Import and Export	
		primary destination		Import and Export	
		secondary destination		Import and Export	
query port	state		enable	Import and Export	
			disable	Import and Export	
telnet command mode	state		enable	Import and Export	
			disable	Import and Export	
	port			Import and Export	
ssh command mode	state		enable	Import and Export	
			disable	Import and Export	
	port			Import and Export	
http server	state		enable	Import and Export	
			disable	Import and Export	
	port			Import and Export	
	secure port			Import and Export	
	max timeout			Import and Export	
	max bytes			Import and Export	
	logging state		enable	Import and Export	

Group Name	Item Name	Value Name	Value	Import/Export	Additional Information
			disable	Import and Export	
	max log entries			Import and Export	
	log format			Import and Export	
serial command mode	mode		disable	Import and Export	
			always	Import and Export	
			cp	Import and Export	
			serial string	Import and Export	
			cp and serial string	Import and Export	
	echo serial string		enable	Import and Export	
			disable	Import and Export	
	serial string			Import and Export	
	signon message			Import and Export	
	wait time			Import and Export	
	cp	group		Import and Export	
		trigger value		Import and Export	
tunnel serial	buffer size			Import and Export	
	read timeout			Import and Export	
	wait read timeout			Import and Export	
tunnel connect	connect mode		enable	Import and Export	
			disable	Import and Export	
			any character	Import and Export	
			start character	Import and Export	
			modem control asserted	Import and Export	
			modem	Import and Export	
	local port			Import and Export	

Group Name	Item Name	Value Name	Value	Import/Export	Additional Information
	remote address			Import and Export	
	remote port			Import and Export	
	protocol		tcp	Import and Export	
			udp	Import and Export	
			ssh	Import and Export	
			tcp aes	Import and Export	
			udp aes	Import and Export	
	reconnect time			Import and Export	
	flush serial		enable	Import and Export	
			disable	Import and Export	
	ssh username			Import and Export	
	block serial		enable	Import and Export	
			disable	Import and Export	
	block network		enable	Import and Export	
			disable	Import and Export	
	tcp keep alive			Import and Export	
	cp set group	cp		Import and Export	
		connection value		Import and Export	
		disconnect value		Import and Export	
tunnel accept	accept mode		enable	Import and Export	
			disable	Import and Export	
			any character	Import and Export	
			start character	Import and Export	
			modem control asserted	Import and Export	
			modem	Import and Export	

Group Name	Item Name	Value Name	Value	Import/Export	Additional Information
	local port			Import and Export	
	protocol		tcp	Import and Export	
			tcp aes	Import and Export	
			ssh	Import and Export	
			telnet	Import and Export	
	flush serial		enable	Import and Export	
			disable	Import and Export	
	block serial		enable	Import and Export	
			disable	Import and Export	
	block network		enable	Import and Export	
			disable	Import and Export	
	tcp keep alive			Import and Export	
	cp set group	cp		Import and Export	
		connection value		Import and Export	
		disconnection value		Import and Export	
tunnel aes accept	encrypt key			Import and Export	
	decrypt key			Import and Export	
tunnel aes connect	encrypt key			Import and Export	
	decrypt key			Import and Export	
tunnel disconnect	disconnect mode		disable	Import and Export	
			timeout	Import and Export	
			stop character	Import and Export	
			modem control not asserted	Import and Export	
	timeout			Import and Export	
		flush serial	enable	Import and Export	

Group Name	Item Name	Value Name	Value	Import/Export	Additional Information
			disable	Import and Export	
tunnel packing	packing mode		disable	Import and Export	
			timeout	Import and Export	
			send character	Import and Export	
	timeout			Import and Export	
	threshold			Import and Export	
	send character			Import and Export	
	trailing character			Import and Export	
tunnel start	start character			Import and Export	
	echo		enable	Import and Export	
			disable	Import and Export	
tunnel stop	stop character			Import and Export	
	echo		enable	Import and Export	
			disable	Import and Export	
tunnel modem	echo pluses		enable	Import and Export	
			disable	Import and Export	
	echo commands		enable	Import and Export	
			disable	Import and Export	
	verbose response		enable	Import and Export	
			disable	Import and Export	
	response type		text	Import and Export	
			numeric	Import and Export	
	error unknown commands		enable	Import and Export	
			disable	Import and Export	
	connect string			Import and Export	
ssh server	host rsa keys	public key		Import and Export	

Group Name	Item Name	Value Name	Value	Import/Export	Additional Information
		private key		Import and Export	
	authorized users	username		Import and Export	
		password		Import and Export	
		public rsa key		Import and Export	
		public dsa key		Import and Export	
	authorized users delete			Import and Export	Delete an SSH authorized user.
	host keys delete			Import and Export	Delete an SSH host key.
ssh client	known host			Import and Export	
		server		Import and Export	
		public rsa key		Import and Export	
	client users	username		Import and Export	
		password		Import and Export	
		remote command		Import and Export	
		public rsa key		Import and Export	
		private rsa key		Import and Export	
		public dsa key		Import and Export	
		private dsa key		Import and Export	
	known host delete			Import and Export	Specify the server host for deletion.
	client users delete			Import and Export	Specify the username for deletion.
	client rsa key delete			Import and Export	Specify the username.
	client dsa key delete			Import and Export	Specify the username.
ssl	certificate	certificate		Import and Export	Enter the text of the certificate.
		private key		Import and Export	Enter the text of the private key.
	delete		certificate	Import and Export	Deletes the current SSL certificate.
rss	feed		enable	Import and Export	
			disable	Import and Export	

Group Name	Item Name	Value Name	Value	Import/Export	Additional Information
	persist		enable	Import and Export	
			disable	Import and Export	
	max entries			Import and Export	
http authentication uri	realm			Import and Export	Attribute of "instance" specifies the uri.
	type			Import and Export	
	user	username		Import and Export	
		password		Import and Export	
	user delete			Import	Delete the HTTP Authentication URI user. The value element is used to specify the user for deletion.
	uri delete			Import	Delete the HTTP Authentication URI. The value of the element is used to specify the URI for deletion.
device	cpu speed			Import and Export	
	short name			Import and Export	
	long name			Import and Export	
ip filter	filter entry	ip address		Import and Export	Delete an IP filter entry.
		net mask		Import and Export	
	filter delete	ip address		Import	
		net mask		Import	
firmware	version			Export	
icmp	state		enable	Import and Export	
			disable	Import and Export	
tcp	resets		enable	Import and Export	
			disable	Import and Export	
ppp	state		enable	Import and Export	
			disable	Import and Export	
	local ip			Import and Export	

Group Name	Item Name	Value Name	Value	Import/Export	Additional Information
	peer ip			Import and Export	
	network mask			Import and Export	
	authentication mode			Import and Export	
	username			Import and Export	
	password			Import and Export	
cp	cp	type	input	Import and Export	
			output	Import and Export	
			nonpio	Import and Export	
		assert low	enable	Import and Export	
			disable	Import and Export	
cp group	set			Import	Set group named by "instance" attribute to the value.
	cp delete			Import	Delete a CP from a group. Specify the cp to delete in the value element.
	group delete			Import	Delete the CP group from the configuration. Specify the group to delete in the value element.
exit cli	state		enable	Import	
			disable	Import	
process method	method		pair	Import	Process the test/set functions as pairs. For each XML item, process the test function then the set function (if the test passed). If a test fails, continue by processing the next item's test function.
			group	Import	Process the test/set functions as a group of tests, then as a group of sets. For each XML Item, process all test functions (before processing any set functions). Then process all the set functions. If a test functions fails, immediately abort.

Group Name	Item Name	Value Name	Value	Import/Export	Additional Information
level passwords	passwords	system		Import	This group specifies the passwords to use when importing an XCR using the CLI capture feature. The system value specifies the root password used if the root level is password protected. Passwords are not required if the CLI is already logged in to the system level.
		enable		Import	The enable value specifies the enable level password to use if the enable level is password-protected. The password is not needed if the CLI is already logged in to the enable level.

12: Branding the XPort AR

The XPort AR's Web Manager and Command Mode (CLI) are customizable.

Web Manager Customization

Customize the Web Manager's appearance by modifying the following files:

Note: *To view these files, open the **http** → **config** folder using the Filesystem Browser. Alternatively, upload and download the files using FTP/TFTP. For more on the filesystem, see Filesystem Configuration on page 56.*

Filename	Description
index.css	The Web Manager's style sheet.
footer.html	Formats the web page's footer.
header.html	Formats the web page's header.
ltrx_logo.gif	The Lantronix logo within the header. To replace the logo, ensure the replacement logo's height is 70 pixels.
bg.gif	The background image file. The background is tiled.

Command Mode

Customize the XPort AR's Command Mode by changing its short name and long name. The short name is used for show commands:

```
(enable)# show XPort AR
```

The long name appears in the Product Type field:

```
(enable)# show XPort AR
Product Information:
       Product Type: Lantronix XPort AR
```

To change the XPort AR's short and long names:

1. Click **System** from the navigation menu. The System window opens.

1. In the **Short Name** field, enter the new short name for the device, up to 8 characters.

2. In the **Long Name** field, enter the new long name for the device.

3. Click **Submit.**

4. To apply changes, click **Reboot**.

13: Updating Firmware

Obtaining Firmware

Obtain the most up-to-date firmware and release notes for the unit from the Lantronix Web site (http://www.lantronix.com/) or by using anonymous FTP (ftp://ftp.lantronix.com/).

Loading New Firmware

Reload the firmware using the XPort AR's Web Manager's System window.

To upload new firmware:

1. Click **System** from the navigation menu. The System window opens.
2. Click in the **Upload New Firmware** section, click **Browse**. A pop-up window displays; locate the firmware file.
3. Click **Upload** to install the firmware on the XPort AR. The device automatically reboots upon the installation of new firmware.

A: Technical Support

If you are experiencing an error that is not described in this user guide, or if you are unable to fix the error, you may:

- Check our online knowledge base at http://www.lantronix.com/support.
- Contact Technical Support in the US:

  Phone: 800-422-7044 (US only) or 949-453-7198

  Fax: 949-450-7226

  Our phone lines are open from 6:00AM - 5:30 PM Pacific Time Monday through Friday, excluding holidays.
- Contact Technical Support in Europe, Middle East, and Africa:

  Phone: +49 (0) 89 31787 817

  Email: eu_techsupp@lantronix.com

Firmware downloads, FAQs, and the most up-to-date documentation are available at: http://www.lantronix.com/support.

When you report a problem, please provide the following information:

- Your name, and your company name, address, and phone number
- Lantronix model number
- Lantronix serial number
- Software version (on the first screen shown when you Telnet to port 9999)
- Description of the problem
- Debug report (stack dump), if applicable
- Status of the unit when the problem occurred (please try to include information on user and network activity at the time of the problem)

B: Binary to Hexadecimal Conversions

Many of the unit's configuration procedures require you to assemble a series of options (represented as bits) into a complete command (represented as a byte). The resulting binary value must be converted to a hexadecimal representation.

Use this chapter to learn to convert binary values to hexadecimals or to look up hexadecimal values in the tables of configuration options. The tables include:

- Command Mode (serial string sign-on message)
- AES Keys

Converting Binary to Hexadecimal

Following are two simple ways to convert binary numbers to hexadecimal notation.

Conversion Table

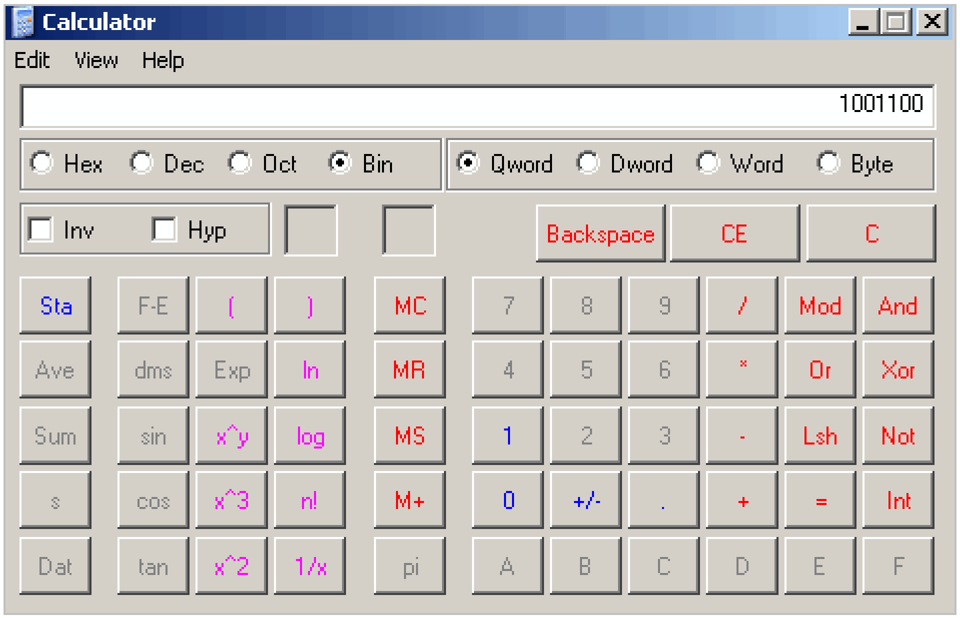
Hexadecimal digits have values ranging from 0 to F, which are represented as 0-9, A (for 10), B (for 11), etc. To convert a binary value (for example, 0100 1100) to a hexadecimal representation, treat the upper and lower four bits separately to produce a two-digit hexadecimal number (in this case, 4C). Use the following table to convert values from binary to hexadecimal.

Decimal	Binary	Hex
0	0000	0
1	0001	1
2	0010	2
3	0011	3
4	0100	4
5	0101	5
6	0110	6
7	0111	7
8	1000	8
9	1001	9
10	1010	A
11	1011	B
12	1100	C
13	1101	D
14	1110	E
15	1111	F

Scientific Calculator

Another simple way to convert binary to hexadecimals is to use a scientific calculator, such as the one available on Windows' operating systems. For example:

1. On the Windows' Start menu, click **Programs→Accessories→Calculator**.
1. On the View menu, select **Scientific**. The scientific calculator displays.
2. Click **Bin** (Binary), and type the number you want to convert.



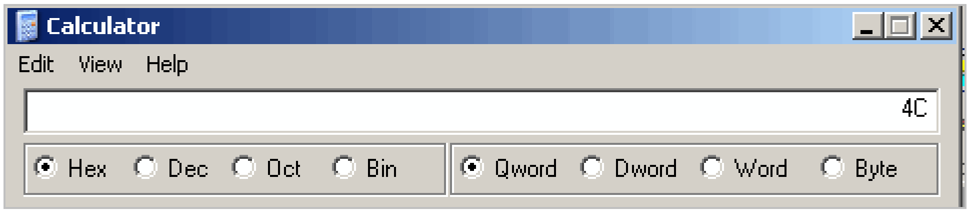
1001100

○ Hex ○ Dec ○ Oct ● Bin

● Qword ○ Dword ○ Word ○ Byte

☐ Inv ☐ Hyp

3. Click **Hex**. The hexadecimal value displays.



4C

● Hex ○ Dec ○ Oct ○ Bin

● Qword ○ Dword ○ Word ○ Byte

Compliance Information

(according to ISO/IEC Guide 22 and EN 45014)

Manufacturer's Name & Address:
Lantronix 15353 Barranca Parkway, Irvine, CA 92618 USA

Declares that the following product:

Product Name Model: Device Server PRODUCT NAME

Conforms to the following standards or other normative documents:

Radiated and conducted emissions
Class B limits of EN 55022:1998
EN55024: 1998 + A1: 2001

Direct & Indirect ESD
EN61000-4-2: 1995

RF Electromagnetic Field Immunity
EN61000-4-3: 1996

Electrical Fast Transient/Burst Immunity
EN61000-4-4: 1995

Surge Immunity
EN61000-4-5: 1995

RF Common Mode Conducted Susceptibility
EN61000-4-6: 1996

Power Frequency Magnetic Field Immunity
EN61000-4-8: 1993

Voltage Dips and Interrupts
EN61000-4-11: 1994

Manufacturer's Contact:
Director of Quality Assurance, Lantronix
15353 Barranca Parkway, Irvine, CA 92618 USA
Tel: 949-453-3990
Fax: 949-453-3995

Warranty

Lantronix warrants each Lantronix product to be free from defects in material and workmanship for a period of **TWO YEARS** after the date of shipment. During this period, if a customer is unable to resolve a product problem with Lantronix Technical Support, a Return Material Authorization (RMA) will be issued. Following receipt of an RMA number, the customer shall return the product to Lantronix, freight prepaid. Upon verification of warranty, Lantronix will -- at its option -- repair or replace the product and return it to the customer freight prepaid. If the product is not under warranty, the customer may have Lantronix repair the unit on a fee basis or return it. No services are handled at the customer's site under this warranty. This warranty is voided if the customer uses the product in an unauthorized or improper way, or in an environment for which it was not designed.

Lantronix warrants the media containing its software product to be free from defects and warrants that the software will operate substantially according to Lantronix specifications for a period of **60 DAYS** after the date of shipment. The customer will ship defective media to Lantronix. Lantronix will ship the replacement media to the customer.

* * * *

In no event will Lantronix be responsible to the user in contract, in tort (including negligence), strict liability or otherwise for any special, indirect, incidental or consequential damage or loss of equipment, plant or power system, cost of capital, loss of profits or revenues, cost of replacement power, additional expenses in the use of existing software, hardware, equipment or facilities, or claims against the user by its employees or customers resulting from the use of the information, recommendations, descriptions and safety notations supplied by Lantronix. Lantronix liability is limited (at its election) to:

refund of buyer's purchase price for such affected products (without interest)

repair or replacement of such products, provided that the buyer follows the above procedures.

There are no understandings, agreements, representations or warranties, express or implied, including warranties of merchantability or fitness for a particular purpose, other than those specifically set out above or by any existing contract between the parties. Any such contract states the entire obligation of Lantronix. The contents of this document shall not become part of or modify any prior or existing agreement, commitment or relationship.

For details on the Lantronix warranty replacement policy, go to our web site at http://www.lantronix.com/support/warranty/index.html